Cours d'arithmétique

Baccalauréat ++

Mohamed ATOUANI

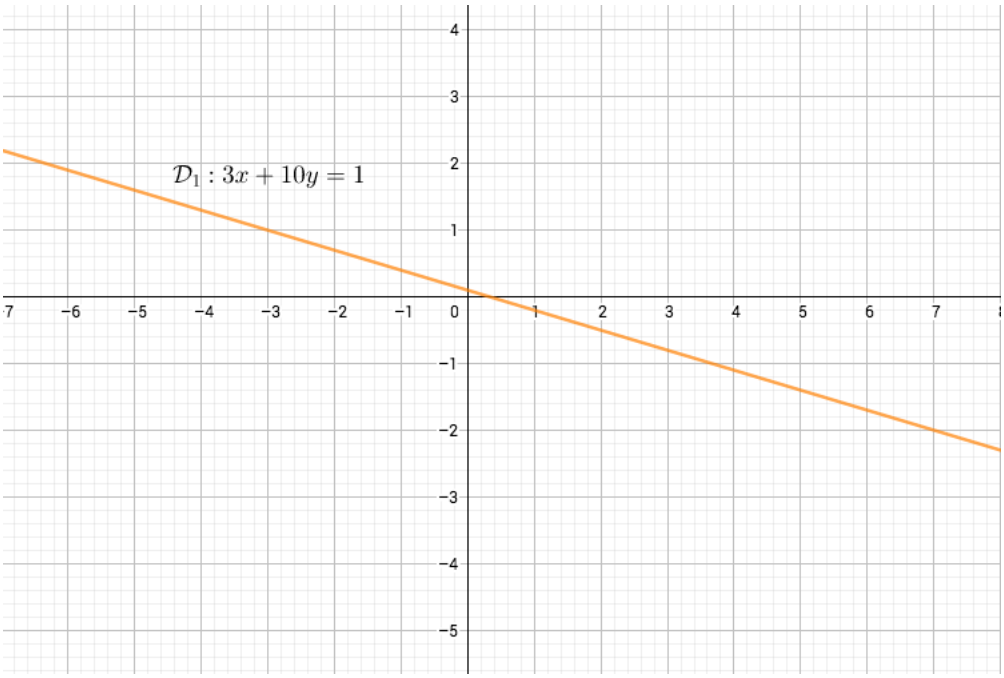
Professeur de Mathématiques
Clandestines

Table des matières

1 Arithmétique sur les droites affines

Nous nous intéressons dans cette première section aux équations diophantiennes de degré 1, à savoir celles de la forme $ax + by = c$, où a, b et c sont des éléments de $\mathbb{Z}$. Les inconnues dans cette histoire sont évidemment x et y et notre objectif est donc de trouver tous les couples d'entiers (x, y) vérifiant l'équation diophantienne. Cette question a un lien direct avec la géométrie, puisque dans le plan, l'équation $ax + by = c$ est celle d'une droite affine. La recherche de couples d'entiers solutions de $ax + by = c$ revient donc à localiser les points à coordonnées entières situés sur la droite de cette même équation. Un exemple vaut bien mieux qu'un long discours.

Exemple 1 : Soit $\mathscr{D}_1$ la droite d'équation $3x + 10y = 1$. On souhaite trouver les points à coordonnées entières situés sur $\mathscr{D}_1$.



Une petite recherche à l'œil nu montre que par exemple le point $(-3, 1)$ est un point à coordonnées entières sur notre droite. Autrement dit, le couple $(-3, 1)$ est solution de l'équation diophantienne $3x + 10y = 1$. Pour s'en convaincre, un petit calcul algébrique montre bien que

$$3 \times (-3) + 10 \times 1 = 1.$$

Super ! Notez toutefois que $(-3, 1)$ n'est pas le seul point à coordonnées entières habitant sur la droite $\mathscr{D}_1$, puisqu'elle passe aussi par le point $(7, -2)$. La question toute naturelle que l'on peut donc se poser ici est : y-a-t-il d'autres points intégrals (un autre mot pour dire à coordonnées entières) situés sur $\mathscr{D}_1$? La réponse est oui et il en existe d'ailleurs une infinité. En effet, en tâtonnant on peut voir que les points intégrals visibles sur la droite sont par exemple lié par la formule

$$x = 10k - 3 \quad \text{et} \quad y = -3k + 1,$$

où k désigne un entier. En prenant $k = 0$, on voit que cette formule donne le point $(-3, 1)$. Pour $k = 1$, on obtient bien le point $(7, -2)$ et pour $k = -1$, on obtient le couple $(-13, 4)$ et

l'on peut vérifier aisément qu'il appartient bien à notre droite car, tout simplement

$$3 \times (-13) + 10 \times 4 = -39 + 40 = 1.$$

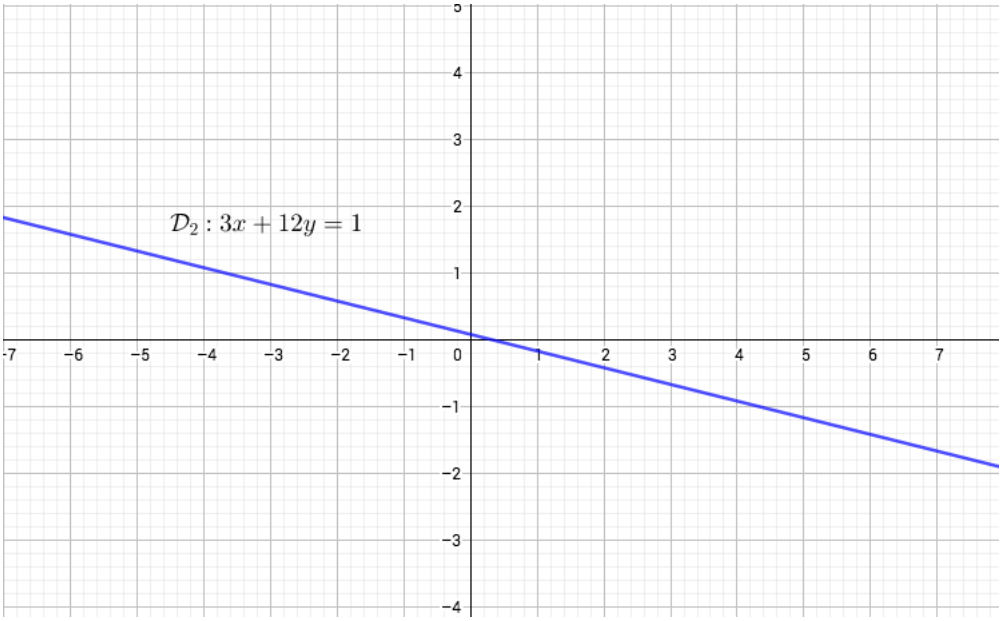
On peut bien sûr vérifier notre formule pour tout entier k, ainsi tout couple de la forme $(10k-3, -3k+1)$ est solution de l'équation diophantienne $3x + 10y = 1$ car

$$3 \times (10k-3) + 10 \times (-3k+1) = 30k - 9 - 30k + 10 = 1.$$

À partir de ce résultat, on peut affirmer qu'il existe une infinité de points à coordonnées entières appartenant à la droite $\mathscr{D}_1$, s'écrivant sous la forme $(10k-3, -3k+1)$. La question toute naturelle serait donc : obtient-on absolument tous les points intégrals habitant sur notre droite en utilisant cette formule ? Autrement dit, existe-il des points à coordonnées entières qui ne s'écrivent pas sous cette forme et qui sont quand même situés sur cette droite ? La réponse est non et l'on pourra affirmer ceci bientôt car cela nécessite quelques connaissances de plus en arithmétique.

Puisqu'on se pose beaucoup de questions ici, une petite dernière avant de terminer cette première section est la suivante : Les droites affines à coefficients entiers croisent-elles toujours des points à coordonnées entières dans le plan ? La réponse est non comme le montre l'exemple ci-dessous.

Exemple 2 : Soit $\mathscr{D}_2$ la droite d'équation $3x + 12y = 1$.



Vous pouvez passer quelques heures à chercher des points à coordonnées entières sur cette droite, vous n'en trouverez pas. L'impossibilité d'un tel fait découle d'une propriété arithmétique des coefficients de la droite $\mathscr{D}_2$. En effet, s'il exite un couple d'entiers (x, y) vérifiant $3x + 12y = 1$ alors $3(x + 4y) = 1$, ce qui signifie que 3 divise 1 (car $x + 4y \in \mathbb{Z}$). Ceci conduit bien évidemment à une contradiction, d'où le résultat.

2 Arithmétique sur le cercle unité

Nous avons aborder dans la première section l'arithmétique sur une droite affine. La droite étant la figure géométrique la plus *simple*, rien ne nous empêche d'étudier l'arith-

métique sur des figures géométriques plus élaborées. Dans cette section, nous allons nous intéresser au cercle unité d'équation $x^2+y^2=1$. Faire de l'arithmétique sur ce cercle signifie qu'on va chercher les points à coordonnées entières sur celui-ci mais pas seulement, nous allons localiser tous les points à coordonnées rationnelles vivant dessus. Un point rationnel est comme son nom l'indique un point dont les coordonnées sont des fractions. Cette recherche conduira à des résultats bien spectaculaires permettant de résoudre le problème le plus ancien des mathématiques, à savoir celui des *triplets pythagoriciens*.

Ainsi, nous souhaitons trouver tous les triplets d'entiers (x,y,z) tels que

$$x^2+y^2=z^2.$$

Cette fameuse équation est bien évidemment en lien avec le fameux théorème de *Pythagore*, auquel cas, sa résolution sur $\mathbb{N}$ signifie qu'on a trouvé un triangle rectangle dont les trois côtés sont des entiers. Notez tout d'abord qu'on peut prendre x et y des entiers arbitraires pour former un triangle rectangle, mais que rien ne garantit que l'hypoténuse z sera entier. Par exemple si $x=3$ et $y=5$, l'équation de Pythagore donne

$$z^2=x^2+y^2=3^2+5^2=34.$$

L'entier 34 n'est pas un carré parfait donc z ne peut pas être un entier. On voit ainsi que la résolution de cette équation avec x,y et z des entiers n'est pas tâche triviale. Le triplet pythagoricien le plus connu du grand public est $(3,4,5)$ car on a $3^2+4^2=5^2$ (vérifier l'égalité seul). Existe-t-il alors d'autres triangles rectangles dont les côtés sont des entiers ? La réponse est oui et là encore il en existe une infinité. En effet, on peut en déduire une infinité à partir du triplet $(3,4,5)$ en agrandissant chacun des côtés par le même facteur k. Pour $k=2$ on obtient le triplet $(6,8,10)$ et on a bien $6^2+8^2=10^2$ car en factorisant par 2^2 cette égalité devient

$$2^2\times 3^2+2^2\times 4^2=2^2\times 5^2,$$

qui est équivalente donc à l'égalité $3^2+4^2=5^2$. Plus généralement, le triplet $(3k,4k,5k)$ est un triplet pythagoricien et ceci est une simple vérification car

$$(3k)^2+(4k)^2=k^2\times(3^2+4^2)=k^2\times 5^2=(5k)^2.$$

On peut alors se demander si tous les triplets pythagoriciens s'obtiennent de cette manière, la réponse est non. En effet, par exemple le triplet $(11,60,61)$ vérifie l'équation de Pythagore et on peut s'en rendre compte sans trop de calculs avec les équivalences suivantes

$$\begin{aligned}
11^2+60^2=61^2 &\iff 11^2=61^2-60^2\\
&\iff 11^2=(61-60)(61+60)\\
&\iff 11^2=1\times 121\\
&\iff 11^2=121.
\end{aligned}$$

La dernière égalité étant une trivialité, le résultat en découle. On voit aisément alors que $(11,60,61)$ n'est pas dérivé du triplet $(3,4,5)$ car par exemple 61 n'est pas multiple de 5. Les triplets que l'on ne peut pas obtenir à partir d'autres triplets s'appellent *triplets primitifs*, combien a-t-on donc de triplets primitifs dans la nature et comment peut-on tous les localiser ? Euclide a répondu à cette question en développant au passage la théorie de la divisibilité qu'on verra ensemble dans ce cours. Toutefois, nous allons présenter ici une méthode géométrique, d'une grande ingéniosité, due à son excellence Diophante d'Alexandrie.

Ainsi, pour résoudre l'équation $x^2+y^2=z^2$, notre ancêtre distingue deux cas :

1er cas : Si $z=0$ alors $x^2+y^2=0$ ce qui implique que $0\leq x^2\leq x^2+y^2=0$ donc que $x^2=0$ ou encore que $x=0$. Par conséquent $y=0$ et dans ce cas ($z=0$) on obtient le triplet trivial $(0,0,0)$.

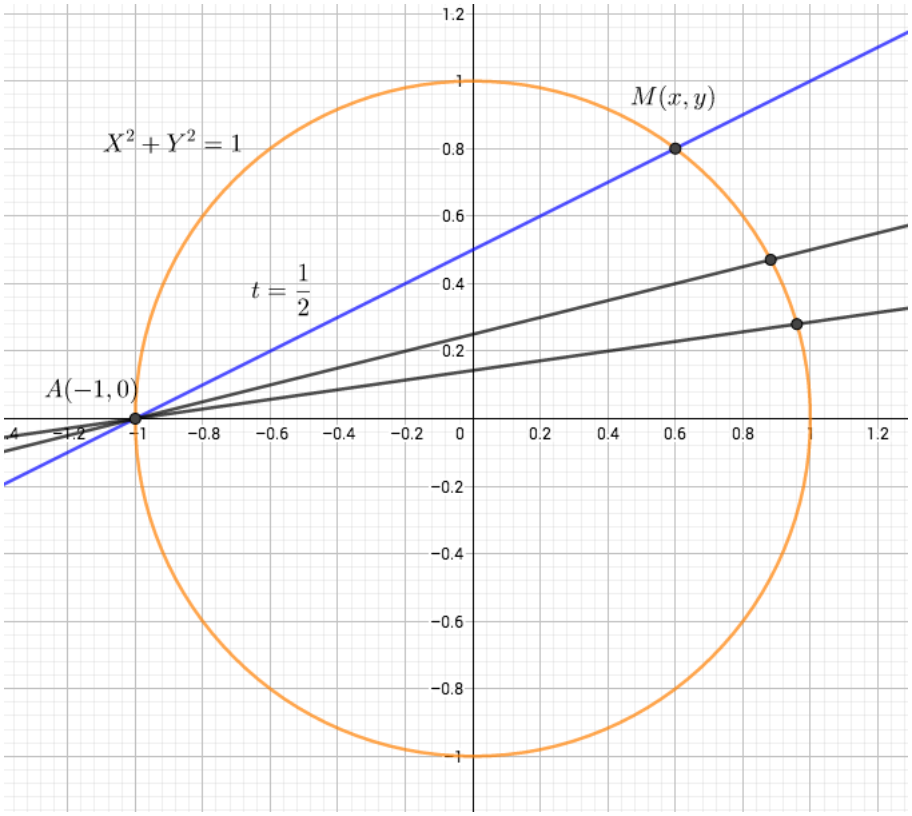
2ème cas : Si $z\neq 0$ alors

$$\begin{aligned} x^2+y^2=z^2 &\iff z^2\left(\frac{x^2}{z^2}+\frac{y^2}{z^2}\right)=z^2\\ &\iff \left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2=1. \end{aligned}$$

On voit donc que (x,y,z) est un triplet pythagoricien si et seulement si le point $M(x/z,y/z)$ est un point à coordonnées rationnelles appartenant au cercle unité d'équation $X^2+Y^2=1$. Réciproquement et c'est facile à vérifier, tout point à coordonnées rationnelles situé sur le cercle unité représente un triplet pythagoricien. Diophante dit alors que la recherche de triplets pythagoriciens revient à la recherche de points à coordonnées rationnelles habitant le cercle unité. Notre problème arithmétique se transforme ainsi en un problème géométrique. Néanmoins, on a l'impression qu'on n'a fait que déplacer le problème, car il n'est pas évident de trouver les points rationnels sur notre emblématique figure géométrique. En effet, on peut prendre X un nombre rationnel mais rien ne garantit que Y le sera. Par exemple si $X=1/2$ alors l'équation $X^2+Y^2=1$ implique que

$$Y^2=1-X^2=1-\left(\frac{1}{2}\right)^2=\frac{3}{4},$$

d'où $Y=\pm\sqrt{3}/2$ qui n'est pas rationnel.



Diophante remarque l'existence de points rationnels triviaux sur le cercle unité dont le point $A(-1,0)$, comme le montre la figure ci-dessus. Il dit alors que la droite passant par A et de cœfficient directeur un nombre rationnel t doit croiser le cercle en un deuxième point de coordonnées rationnelles. Il suffit alors de résoudre un couple d'équations afin de localiser ce fameux deuxième point. Diophante prétend qu'on peut obtenir tous les points rationnels de cette manière en faisant varier le rationnel t. Essayons ce procédé avec un exemple concret.

Exemple : Soit $t = 1/2$. La droite $D_{1/2}$ passant par $A(-1,0)$ et de pente égale à t est d'équation $y = t(x+1) = 1/2(x+1)$ (pourquoi ?). Le point $M(x,y)$, le deuxième point d'intersection de $D_{1/2}$ et du cercle unité, vérifie donc le système d'équation

$$\begin{cases} y = \frac{1}{2}(x+1) \\ x^2 + y^2 = 1 \end{cases}$$

En substituant la première équation dans la deuxième on obtient l'équation du second degré en x

$$x^2 + \left(\frac{1}{2}(x+1)\right)^2 = 1.$$

Pas besoin d'appliquer un *delta* ici, il suffit de remarquer que l'équation se factorise trivialement de la façon suivante

$$\begin{aligned} x^2 + \left(\frac{1}{2}(x+1)\right)^2 = 1 &\iff x^2 - 1 + \frac{1}{4}(x+1)^2 = 0 \\ &\iff (x-1)(x+1) + \frac{1}{4}(x+1)^2 = 0 \\ &\iff (x+1)\left(x - 1 + \frac{1}{4}(x+1)\right) = 0 \\ &\iff (x+1)\left(\frac{5}{4}x - \frac{3}{4}\right) = 0 \\ &\iff x = -1 \quad \text{ou} \quad x = \frac{3}{5}. \end{aligned}$$

La solution $x = -1$ est tout à fait normale car je vous rappelle qu'on est à la recherche des points d'intersection de la droite $D_{1/2}$ et du cercle unité. Le premier point est A qui est d'abscisse $x = -1$, le deuxième point est donc d'abscisse égale à $x = 3/5$. Son ordonnée est donnée par la formule

$$y = \frac{1}{2}(x+1) = \frac{1}{2}\left(\frac{3}{5} + 1\right) = \frac{4}{5}.$$

Le point M est donc de coordonnées $(3/5, 4/5)$, qui est un point à coordonnées rationnelles appartenant au cercle unité. Cela implique en particulier que ses coordonnées vérifient l'équation du cercle, à savoir

$$\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1,$$

en multipliant de part et d'autre par 5^2 on obtient $3^2 + 4^2 = 5^2$. Bingo ! ! ! On a pu localiser un premier triplet pythagoricien. La méthode suggère que si on fait varier la pente t, on obtiendra davantage de triplets pythagoriciens. Ainsi, nous allons faire le même procédé

mais cette fois avec un t quelconque.

Soit donc $t \in \mathbb{Q}$. La droite D_t de pente t et passant par $A(-1,0)$ a pour équation $y = t(x+1)$. Les coordonnées du deuxième point d'intersection de D_t et du cercle unité vérifient le système d'équations

$$\begin{cases} y = t(x+1) \\ x^2 + y^2 = 1 \end{cases}$$

La substitution de la première équation dans la deuxième donne

$$\begin{aligned} x^2 + \big(t(x+1)\big)^2 = 1 &\iff x^2 - 1 + t^2(x+1)^2 = 0 \\ &\iff (x-1)(x+1) + t^2(x+1)^2 = 0 \\ &\iff (x+1)\big(x - 1 + t^2(x+1)\big) = 0 \\ &\iff x = -1 \quad \text{ou} \quad x = \frac{1-t^2}{1+t^2}. \end{aligned}$$

De même, l'ordonnée du deuxième point d'intersection est donnée par la formule

$$y = t(x+1) = t\left(\frac{1-t^2}{1+t^2} + 1\right) = \frac{2t}{1+t^2}.$$

Le point M est donc de coordonnées $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, son appartenance au cercle unité implique que

$$\left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 = 1.$$

Or t est un nombre rationnel, donc s'écrit sous la forme $t = u/v$ où u et v sont deux entiers. En substituant on obtient

$$\left(\frac{1-(u/v)^2}{1+(u/v)^2}\right)^2 + \left(\frac{2(u/v)}{1+(u/v)^2}\right)^2 = 1$$

Pas peur d'effectuer des simplifications, on multiplie chacune des fractions en haut et en bas par v^2 pour obtenir la relation

$$\left(\frac{v^2-u^2}{v^2+u^2}\right)^2 + \left(\frac{2uv}{v^2+u^2}\right)^2 = 1.$$

En multipliant maintenant de part et d'autre par $(v^2+u^2)^2$ on obtient la fameuse formule donnant tous les triplets pythagoriciens, à savoir

$$\boxed{(v^2-u^2)^2 + (2uv)^2 = (u^2+v^2)^2.}$$

Convaincu ? Non ! ! Prenons $u = 5$ et $v = 6$. La formule donne l'égalité $(6^2-5^2)^2 + (2\times 5\times 6)^2 = (6^2+5^2)^2$, ou encore

$$11^2 + 60^2 = 61^2 !!!$$

On retombe ici sur le triplet $(11, 60, 61)$. Incroyable !

Remarques :

1. On peut démontrer facilement l'exactitude de la formule générant tous les triplets pythagoriciens et ce en développant tout simplement les deux expressions à droite et à gauche de l'égalité. Toutefois, ce qui est difficile, c'est d'imaginer une telle formule. L'idée géniale de Diophante a permis de l'établir, sans trop d'efforts.

2. Pourquoi cette formule donne-t-elle tous les triplets pythagoriciens ? La justification est relativement simple : toute droite D_t de pente rationnelle donne un point rationnel sur le cercle représentant un triplet pythagoricien. Réciproquement, si $M(x,y)$ est un point rationnel sur le cercle unité (différent de A bien sûr) alors la droite passant par M et par notre fameux point A est forcément de pente rationnelle (pourquoi ?).

3. Après calcul, on voit que le deuxième point d'intersection de D_t et du cercle unité est un point à coordonnées rationnelles. Cette observation est la clef de notre petite théorie, sans quoi tout tombe à l'eau. Y-a-t-il une raison plus théorique à ce fait ? En effet, le système d'équations à résoudre conduit à une équation du second degré en x sous la forme $x^2+px+q=0$, où $p,q\in\mathbb{Q}$. Notons alors que si x_1,x_2 sont deux solutions à celle-ci alors

$$x^2+px+q=(x-x_1)(x-x_2)=x^2-(x_1+x_2)x+x_1x_2.$$

   Par identification, on obtient par exemple que $-p=x_1+x_2$. Cela implique en particulier que si $x_1\in\mathbb{Q}$ alors $x_2=-p-x_1\in\mathbb{Q}$. Le résultat tombe donc comme la pomme de Newton.

3 Arithmétique sur l'hyperbole et approximations rationnelles

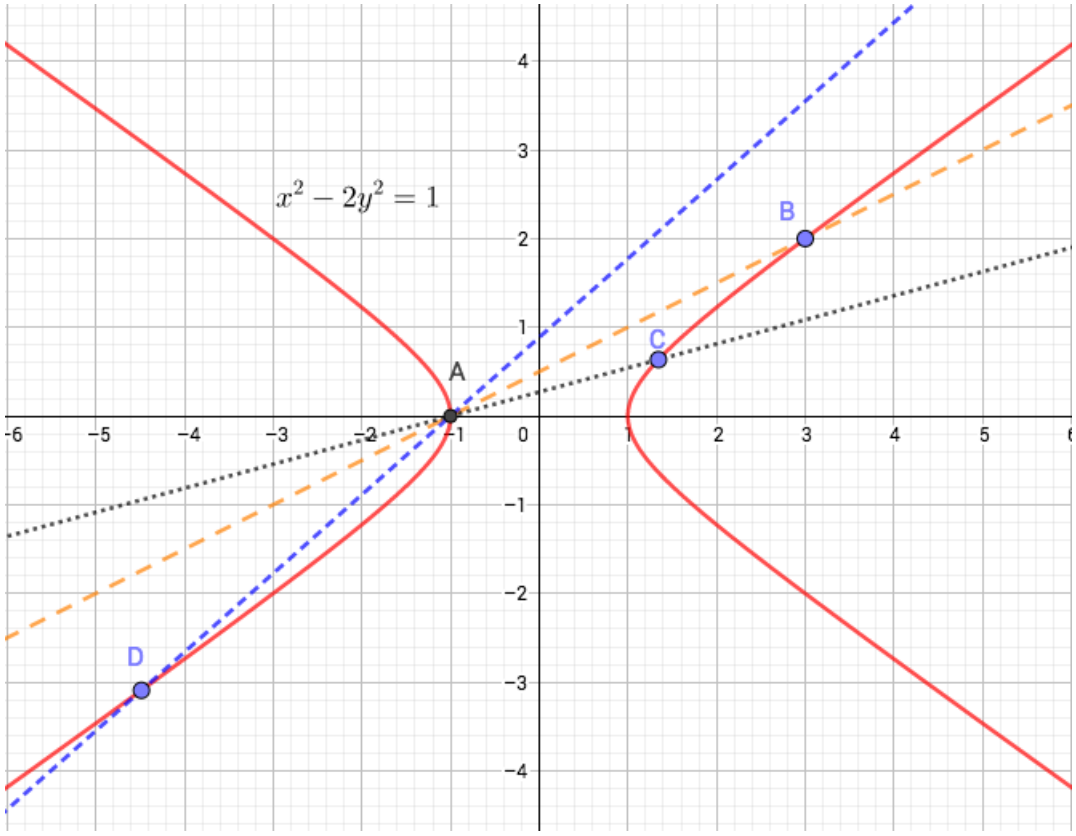
Nous avons abordé dans les deux premières sections l'arithmétique sur les droites affines et l'arithmétique sur le cercle unité, nous aborderons dans cette partie l'arithmétique sur l'hyperbole d'équation $x^2-2y^2=1$. Nous verrons que l'étude des points à coordonnées entières sur cet objet géométrique permet de mieux approcher le fameux irrationnel $\sqrt{2}$.

L'équation diophantienne $x^2-2y^2=1$ est un cas particulier des équations dites de Pell $x^2-ny^2=1$, où n n'est pas un carré parfait. Le cas des carrés parfaits est relativement trivial. En effet, si $n=m^2$, l'équation de notre regretté Pell (en réalité Pell n'est pas le mathématicien à l'origine de l'étude de ce type d'équation, mais ceci est une autre histoire) devient

$$\begin{aligned} x^2-ny^2=1 &\iff x^2-m^2y^2=1\\ &\iff (x-my)(x+my)=1. \end{aligned}$$

Cela signifie en particulier que $x-my=1$ et $x+my=1$ ou $x-my=-1$ et $x+my=-1$, car il s'agit de diviseurs de 1. Dans le premier cas seul le couple $(1,0)$ est solution et dans le deuxième cas il s'agit de $(-1,0)$ (pourquoi ?). D'où notre affirmation. La question devient nettement plus difficile quand n n'est pas un carré parfait.

Nous commençons par inspecter les points rationnels situés sur l'hyperbole, en utilisant la méthode de la corde de Diophante. En effet, sur la figure ci-dessous, on voit que le point A de coordonnées $(-1,0)$ est un point trivial à coordonnées rationnelles vérifiant l'équation $x^2-2y^2=1$.



Soit $t \in \mathbb{Q}$. La droite D_t de pente t et passant par A a pour équation $y = t(x+1)$. Les coordonnées du deuxième point d'intersection de D_t avec l'hyperbole vérifient le système d'équations

$$\begin{cases} y = t(x+1) \\ x^2-2y^2=1 \end{cases}$$

En subsituant la première équation dans la deuxième on obtient l'équation du second degré en x

$$x^2-2\big(t(x+1)\big)^2=1.$$

Là encore, nous n'avons pas besoin d'appliquer la fameuse formule du *delta* [1] car

$$\begin{aligned} x^2-2\big(t(x+1)\big)^2=1 &\iff x^2-1-2\big(t(x+1)\big)^2=0 \\ &\iff (x-1)(x+1)-2t^2(x+1)^2=0 \\ &\iff (x+1)\big(x-1-2t^2(x+1)\big) \\ &\iff x=-1 \quad \text{ou} \quad x=\frac{1+2t^2}{1-2t^2}. \end{aligned}$$

1. Passer par le delta cache souvent la mécanique sous-jacente à la résolution d'équations, à utiliser seulement en cas de nécessité.

La division par $1-2t^2$ n'est pas illicite ici car aucun rationnel au carré ne donne $1/2$ ($t^2 \neq 1/2$). L'ordonnée du point recherché est donc donnée par la formule

$$y = t(x+1) = t\left(\frac{1+2t^2}{1-2t^2}+1\right) = \frac{2t}{1-2t^2}.$$

Puisque ce point appartient à l'hyperbole, ses coordonnées vérifient son équation, à savoir

$$\left(\frac{1+2t^2}{1-2t^2}\right)^2 - 2\left(\frac{2t}{1-2t^2}\right)^2 = 1.$$

Notez alors que cette formule est facile à démontrer, mais difficile à imaginer sans la méthode de Diophante. Si $t=0$ (droite horizontale), ma formule devrait me donner le point $(1,0)$, est-ce correct ? Dans ce cas,

$$x = \frac{1+2\times 0^2}{1+2\times 0^2} = 1 \quad \text{et} \quad y = \frac{2\times 0}{1-2\times 0^2} = 0.$$

Super, notre formule donne le bon point pour $t=0$. Pour $t=1/4$ on obtient

$$x = \frac{1+2\times(1/4)^2}{1-2\times(1/4)^2} = \frac{9}{7} \quad \text{et} \quad y = \frac{2\times 1/4}{1-2\times(1/4)^2} = \frac{4}{7}.$$

Le point $(9/7, 4/7)$ vérifie-t-il l'équation $x^2-2y^2=1$? Pour s'en convaincre un petit calcul s'impose

$$\begin{aligned}\left(\frac{9}{7}\right)^2 - 2\times\left(\frac{4}{7}\right)^2 &= \frac{81}{49} - 2\times\frac{16}{49}\\ &= \frac{81-32}{49}\\ &= \frac{49}{49} = 1.\end{aligned}$$

Bingo ! Cela donne bien un point rationnel sur la courbe et on obtient ainsi tous les points rationnels sur celle-ci.

Les points rationnels, c'est bien, mais peut-on en déduire les points à coordonnées entières comme avec le cercle unité ? Les choses sont plus subtiles dans ce cas. En effet, soit $t = u/v$, où $u, v \in \mathbb{Z}$ et $v \neq 0$.

$$\left(\frac{1+2t^2}{1-2t^2}\right)^2 - 2\left(\frac{2t}{1-2t^2}\right)^2 = 1 \iff \left(\frac{1+2(u/v)^2}{1-2(u/v)^2}\right)^2 - 2\left(\frac{2u/v}{1-2(u/v)^2}\right)^2 = 1.$$

En multipliant en haut et en bas chacune des fractions par v^2 on obtient

$$\left(\frac{v^2+2u^2}{v^2-2u^2}\right)^2 - 2\left(\frac{2uv}{v^2-2u^2}\right)^2 = 1.$$

Cette dernière égalité est équivalente à l'égalité

$$\boxed{(v^2+2u^2)^2 - 2(2uv)^2 = (v^2-2u^2)^2}.$$

La méthode de Diophante donne encore une jolie identité, générant tous les points à coordonnées entières sur l'objet géométrique d'équation $x^2-2y^2=z^2$. Je vous rappelle que dans notre cas, on s'intéresse à l'équation $x^2-2y^2=1$, il suffit alors de prendre $z=1$ dans l'identité ci-dessus afin de résoudre l'équation de Pell dans $\mathbb{Z}^2$. Toutefois, la condition $z=1$ est équivalente à $v^2-2u^2=1$!!! Impasse, retour à la case départ car $v^2-2u^2=1$ est la même que $x^2-2y^2=1$. Heureusement que dans notre cas, il existe des solutions entières faciles [2] à trouver par inspection comme le couple $(3,2)$ car

$$3^2-2\times 2^2=1.$$

Il est alors évident que $(\pm 3,\pm 2)$ sont tous solutions de notre équation. Pour des raisons que nous découvrirons sous-peu, nous allons encoder la solution $(3,2)$ dans le nombre réel $3+2\sqrt{2}$. De même, si (a,b) est solution de l'équation $x^2-2y^2=1$, nous considérerons le nombre $a+b\sqrt{2}$. On dit alors que a est la partie rationnelle de la solution et b sa partie irrationnelle [3]. L'irrationalité de $\sqrt{2}$ se traduit par l'unicité de cette représentation. En effet, si a_1,b_1,a_2 et $b_2\in\mathbb{Z}$ tels que

$$a_1+b_1\sqrt{2}=a_2+b_2\sqrt{2},$$

alors $a_1=a_2$ et $b_1=b_2$. Supposons au contraire que $b_1\neq b_2$, on obtient dans ce cas

$$a_1-a_2=(b_2-b_1)\sqrt{2},$$

ce qui implique une contradiction [4], à savoir

$$\sqrt{2}=\frac{a_1-a_2}{b_2-b_1}.$$

On en déduit que $b_1=b_2$ et que par conséquent $a_1=a_2$. Représenter les solutions d'une équation de type $x^2-ny^2=1$ n'est pas possible quand n est un carré parfait. En effet, si $n=4$ alors les couples $(3,1)$ et $(1,2)$ sont représentés par un même nombre puisque

$$3+\sqrt{4}=1+2\sqrt{4}.$$

Venons-en maintenant à l'intérêt de cette écriture. Afin d'obtenir toutes les solutions de l'équation de Pell $x^2-2y^2=1$, il suffit de calculer les puissances successives de $3+2\sqrt{2}$. Nous avons en effet

$$\begin{aligned}(3+2\sqrt{2})^2&=3^2+2\times 3\times 2\sqrt{2}+(2\sqrt{2})^2\\&=17+12\sqrt{2},\end{aligned}$$

le couple $(17,12)$ est bien solution de l'équation car

$$17^2-2\times 12^2=289-288=1!!$$

Maintenant, un petit calcul montre que $(3+2\sqrt{2})^3=99+70\sqrt{2}$ et on a bien $99^2-2\times 70^2=1$ (vérifier les calculs seul). C'est incroyable, il parait que les puissances successives de $3+2\sqrt{2}$

2. Ce n'est pas toujours le cas. Par exemple la première solution positive de l'équation $x^2-61y^2=1$ est (1766319049, 226153980). Bon courage pour trouver ce couple à la main.

3. Il y a une similarité ici avec partie réelle et partie imaginaire des nombres complexes.

4. Je vous rappelle que $\sqrt{2}$ est un nombre irrationnel, donc ne peut pas s'écrire sous la forme d'une fraction. Nous verrons une preuve de cette affirmation plus loin.

encodent bien les solutions entières de notre chère équation. Mais pourquoi ?

Les équations de Pell contiennent une structure bien particulière et nous allons montrer plus généralement que si $a_1 + b_1\sqrt{2}$ et $a_2 + b_2\sqrt{2}$ sont deux solutions alors

$$a_3 + b_3\sqrt{2} = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$$

l'est aussi. En développant l'expression à droite de l'égalité on obtient

$$\begin{aligned} a_3 + b_3\sqrt{2} &= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}. \end{aligned}$$

Pour montrer que (a_3, b_3) est une nouvelle solution, il suffit de montrer que

$$(a_1a_2 + 2b_1b_2)^2 - 2(a_1b_2 + a_2b_1)^2 = 1.$$

Pour se faire, nous procéderons astucieusement. Nous savons en effet que (a_1, b_1) et (a_2, b_2) sont solutions donc

$$a_1^2 - 2b_1^2 = 1 \quad \text{et} \quad a_2^2 - 2b_2^2 = 1,$$

on en déduit en utilisant l'identité remarquable $a^2 - b^2 = (a - b)(a + b)$ que

$$\begin{aligned} 1 &= (a_1^2 - 2b_1^2)(a_2^2 - 2b_2^2) \\ &= (a_1 - b_1\sqrt{2})(a_1 + b_1\sqrt{2})(a_2 - b_2\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= (a_1 - b_1\sqrt{2})(a_2 - b_2\sqrt{2})(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\ &= \big((a_1a_2 + 2b_1b_2) - (a_1b_2 + a_2b_1)\sqrt{2}\big)\big((a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}\big) \\ &= (a_1a_2 + 2b_1b_2)^2 - 2(a_1b_2 + a_2b_1)^2. \end{aligned}$$

La dernière égalité découle elle aussi de la troisième identité remarquable car

$$(a - b\sqrt{2})(a + b\sqrt{2}) = a^2 - 2b^2.$$

Ce raisonnement justifie que les puissances successives de $3 + 2\sqrt{2}$ sont solutions de l'équation de Pell car on a tout simplement multiplié $3 + 2\sqrt{2}$ par lui-même.

Ce qui est encore plus surprenant dans cette histoire, c'est que les points à coordonnées entières situés sur l'hyperbole d'équation $x^2 - 2y^2 = 1$ donnent des renseignements sur les décimales de $\sqrt{2}$. Tout d'abord, notez qu'il est facile de calculer les décimales d'une fraction, en utilisant l'algorithme de division décimale d'Euclide (celui qu'on a appris à l'école primaire). Cet algorithme fort simple et fort sympathique ne s'applique plus à $\sqrt{2}$ car ce dernier est irrationnel. Ce qui est magique avec notre petite étude de l'hyperbole, ses points à coordonnées entières vont fournir des fractions de plus en plus proche de $\sqrt{2}$. Cela permettra donc de trouver ses décimales en utilisant nos connaissances de base sur la division. En effet, la première solution $(3, 2)$ donne la fraction

$$\frac{3}{2} = 1.5,$$

le couple $(17, 12)$ donne la fraction

$$\frac{17}{12} = 1.416666\cdots$$

et le couple $(99,70)$ donne $\frac{99}{70} = 1.4142\cdots$. À vos calculatrices pour voir que cette fraction partage 4 décimales avec $\sqrt{2}$. Je vous invite à calculer d'autres solutions afin de voir que les fractions se rapprochent de plus en plus de notre fameux irrationel. Mais pourquoi ? La raison à cela est là encore relativement triviale car si (x,y) est un point à coordonnées entières sur l'hyperbole et $y \neq 0$ alors l'égalité $x^2 - 2y^2 = 1$ implique en divisant par y^2 que

$$\left(\frac{x}{y}\right)^2 - 2 = \frac{1}{y^2}.$$

Donc si y est suffisamment grand, $1/y^2$ sera proche de 0. Par conséquent

$$\left(\frac{x}{y}\right)^2 - 2 \simeq 0,$$

ou encore $x/y \simeq \sqrt{2}$. Great ! Avant de finir cette section, une question me vient à l'esprit : toute hyperbole croise-t-elle des points à coordonnées entières dans le plan. La réponse est non et cela dépend là encore des propriétés arithmétiques des coefficients de l'équation de celle-ci.

En effet, soit $\mathscr{H}$ l'hyperbole d'équation $x^2 - 5y^2 = 2$. Cette dernière ne contient aucun point à coordonnées entières pour la raison suivante. Si (x,y) est un couple solution de l'équation $x^2 - 5y^2 = 2$ alors on a $x^2 = 2 + 5y^2$. Cela peut se lire "le reste de la division euclidienne de x^2 par 5 vaut 2". Nous allons démontrer que ceci est impossible. Modulo 5, x ne peut être congru qu'à 0, 1, 2, 3 ou 4. Ainsi,

- Si $x \equiv 0 \pmod 5$ alors $x^2 \equiv 0^2 \pmod 5 \equiv 0 \pmod 5 \not\equiv 2 \pmod 5$.
- Si $x \equiv 1 \pmod 5$ alors $x^2 \equiv 1^2 \pmod 5 \equiv 1 \pmod 5 \not\equiv 2 \pmod 5$.
- Si $x \equiv 2 \pmod 5$ alors $x^2 \equiv 2^2 \pmod 5 \equiv 4 \pmod 5 \not\equiv 2 \pmod 5$.
- Si $x \equiv 3 \pmod 5$ alors $x^2 \equiv 3^2 \pmod 5 \equiv 4 \pmod 5 \not\equiv 2 \pmod 5$.
- Si $x \equiv 4 \pmod 5$ alors $x^2 \equiv 4^2 \pmod 5 \equiv 1 \pmod 5 \not\equiv 2 \pmod 5$.

Dans tous les cas, $x^2 \not\equiv 2 \pmod 5$. Le résultat en découle [5].

4 Le principe de récurrence

Nous allons explorer dans cette section le principe de la récurrence via quelques phénomènes sur les entiers naturels.

Exemple 1 : Dans cet exemple, nous nous intéressons à la somme des entiers naturels impairs, à savoir

$$S_n = \sum_{k=1}^{n} (2k-1).$$

5. Cette preuve est élémentaire pour ceux qui connaissent les congruences, sinon nous aborderons cet outil plus loin en détail.

Rien ne vaut une petite expérimentation pour voir que

$$\begin{aligned}
S_1 &= 1 = 1^2\\
S_2 &= \underbrace{1}_{S_1} + 3 = 4 = 2^2\\
S_3 &= \underbrace{1+3}_{S_2} + 5 = 4 + 5 = 9 = 3^2\\
S_4 &= \underbrace{1+3+5}_{S_3} + 7 = 9 + 7 = 16 = 4^2\\
S_5 &= \underbrace{1+3+5+7}_{S_4} + 9 = 16 + 9 = 25 = 5^2\\
&\vdots
\end{aligned}$$

On se rend compte donc que pour les premières valeurs de n, la somme des n premiers entiers naturels impairs vaut n^2, autrement dit $\boxed{S_n = n^2}$. Ce résultat reste-t-il vrai pour tout entier naturel $n \geq 1$? C'est à dire si je m'amuse à prendre $n = 1000$, vais-je obtenir

$$S_{1000} = 1 + 3 + \cdots + 1999 = 1000^2 ?$$

Notre expérimentation avec les cinq premières valeurs de n nous donne une idée sur ce qui devrait se passer à n'importe quel rang n. Toutefois, sans démonstration mathématique, rien ne garantit la validité de notre conjecture. Afin de prouver ce résultat pour tout entier naturel $n \geq 1$, nous allons procéder par récurrence. Remarquons tout d'abord que la somme S_{n+1}, au rang $n+1$, se déduit à partir de la somme S_n, au rang n, par la formule

$$S_{n+1} = S_n + (2n+1).$$

C'est assez trivial puisque

$$\begin{aligned}
S_n &= 1 + 3 + \cdots + (2n-1)\\
S_{n+1} &= 1 + 3 + \cdots + (2n-1) + (2n+1),
\end{aligned}$$

car $(2n+1)$ est l'entier impair suivant $(2n-1)$. Cela suggère que les propriétés de S_{n+1} sont liées aux propriétés de S_n. La récurrence consiste essentiellement à partir de S_n pour prouver S_{n+1}. Pour se faire, notons $\mathscr{P}(n)$ la propriété

$$\mathscr{P}(n) : \quad S_n = n^2.$$

On doit alors vérifier que $\mathscr{P}(1)$ est vraie, étape qu'on appellera **l'initialisation**. Ensuite on doit montrer que si pour un entier naturel n, $\mathscr{P}(n)$ est vraie alors $\mathscr{P}(n+1)$ est vraie aussi. Cette dernière étape s'appelle **l'hérédité**. Puisqu'on a vérifié la véracité de $\mathscr{P}(1)$ et puisqu'on a montré pour un n quelconque que $\mathscr{P}(n) \implies \mathscr{P}(n+1)$, cela donne le schéma

$$\mathscr{P}(1) \underset{HR}{\implies} \mathscr{P}(2) \underset{HR}{\implies} \mathscr{P}(3) \cdots \underset{HR}{\implies} \mathscr{P}(n) \underset{HR}{\implies} \cdots$$

où HR désigne l'hérédité. On comprend alors $\mathscr{P}(1)$ est vraie donc $\mathscr{P}(2)$ est vraie aussi, ce qui implique la véracité de $\mathscr{P}(3)$ etc et tout ceci grâce à l'hérédité. On peut imager la récurrence comme la chute d'une file infinie de dominos comme le montre la figure ci-dessous. Si je suis certain que le premier domino va tomber et si de plus je sais que la chute du n-ème domino entraine la chute du $n+1$-ème domino pour n'importe quel rang n, alors je sais que les dominos vont tomber l'un après l'autre et ce jusqu'à l'infini. L'histoire est la même avec la récurrence !

Revenons à nos moutons et démontrons par récurrence que $S_n = n^2$ pour tout entier naturel $n \geq 1$.

- **Initialisation :** La propriété $\mathscr{P}(1)$ est vraie car

$$S_1 = 1 = 1^2.$$

  Ainsi la formule $S_n = n^2$ s'applique bien pour $n = 1$.

- **Hérédité :** Soit $n \geq 1$ un entier naturel. Supposons que $\mathscr{P}(n)$ est vraie et montrons dans ce cas que $\mathscr{P}(n+1)$ l'est aussi. On sait donc que pour ce n choisi au hasard $S_n = n^2$ et on souhaite prouver que $S_{n+1} = (n+1)^2$. Or on a vu que S_{n+1} et S_n sont liées par la formule $S_{n+1} = S_n + (2n+1)$, cela implique donc que

$$S_{n+1} = n^2 + (2n+1) = (n+1)^2.$$

  D'où le résultat.

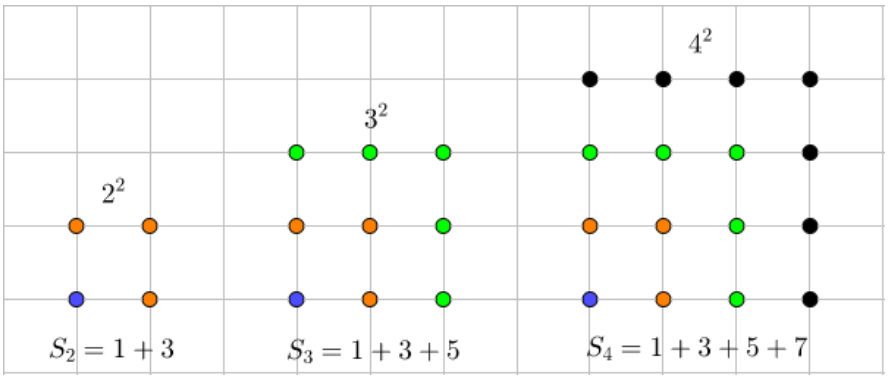
Il existe plusieurs preuves à notre résultat et à vrai dire, la récurrence n'est pas le meilleur moyen pour y arriver. Une deuxième preuve utilise une manipulation algébrique consistant à rajouter tous les entiers pairs et à les soustraire à la fois pour obtenir

$$\begin{aligned}
S_n &= 1+3+\cdots+(2n-1) \\
&= 1+2+3+4+\cdots+(2n-2)+(2n-1)-(2+4+\cdots+(2n-2)) \\
&= 1+2+3+4+\cdots+(2n-2)+(2n-1)-2(1+2+\cdots+(n-1)) \\
&= \frac{(2n-1)(2n-1+1)}{2} - 2\frac{(n-1)(n-1+1)}{2} \\
&= \frac{(2n-1)\times 2n}{2} - n(n-1) \\
&= n(2n-1) - n(n-1) \\
&= n(2n-1-n+1) \\
&= n^2.
\end{aligned}$$

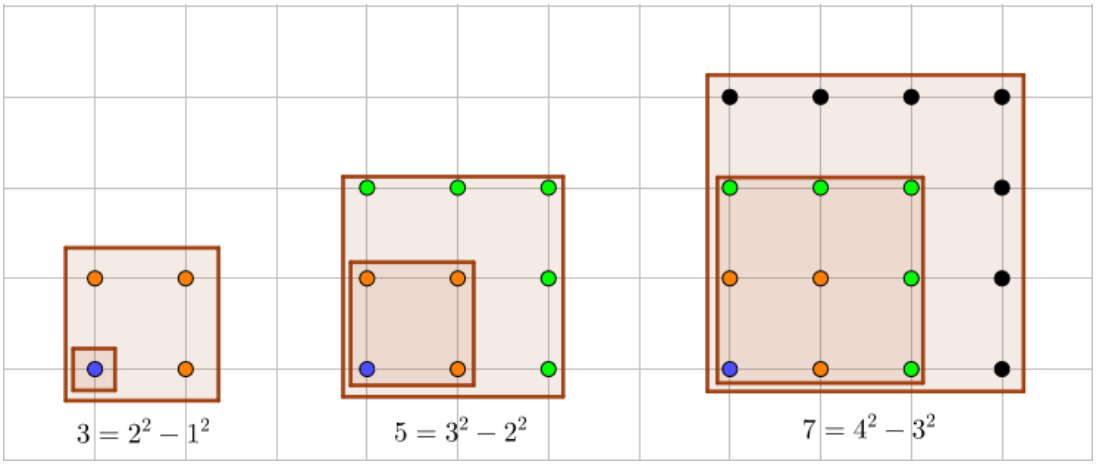
Voilà tout simplement et j'espère que vous avez remarqué qu'on a utilisé le résultat affirmant que la somme des n premiers entiers naturels vaut $n(n+1)/2$. Autrement dit

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}.$$

Avouons que cette astuce sort de l'espace. De surcroît, on ne comprend toujours pas bien pourquoi notre somme donne toujours un carré parfait. Une meilleure approche est de visualiser cette somme géométriquement, comme le montre la figure ci-dessous



Une belle preuve sans mots. Je vous invite à dessiner S_5 et S_6 pour vous en convaincre et voir que la figure finale sera toujours un carré. Notez toutefois que suivant les normes de la rigueur moderne, une visualisation ne vaut jamais une preuve mathématique. Néanmoins, cette figure suggère une preuve algébrique rigoureuse,



à savoir tout entier naturel impair est la différence de deux carrés consécutifs. Sachant que tout entier impair peut s'écrire sous la forme $2k-1$, ce résultat se démontre facilement car

$$k^2-(k-1)^2=k^2-(k^2-2k+1)=2k-1.$$

Notre dulcinée somme S_n devient donc

$$\begin{aligned}S_n&=1+3+5+\cdots+(2n-3)+(2n-1)\\&=(1^2-0^2)+(2^2-1^2)+(3^2-2^2)+\cdots+((n-1)^2-(n-2)^2)+(n^2-(n-1)^2)\\&=(\cancel{1}^2-0^2)+(\cancel{2}^2-\cancel{1}^2)+(3^2-\cancel{2}^2)+\cdots+((n\cancel{-1})^2-(n-2)^2)+(n^2-(n\cancel{-1})^2)\end{aligned}$$

et on voit que tous les termes s'annulent sauf $n^2-0^2=n^2$. Le résultat en découle. Cette preuve, bien plus parlante que les autres, cache en réalité une récurrence dans les trois

points de suspension. En toute rigueur et pour éviter toute confusion, on pourra démontrer par récurrence le résultat plus général sur les sommes télescopiques : si (u_n) est une suite de nombres alors

$$\sum_{k=0}^{n}(u_{k+1}-u_k)=u_{n+1}-u_0.$$

En effet, par récurrence on a

- **Initialisation :** Si $n=0$ alors

$$\sum_{k=0}^{0}(u_{k+1}-u_k)=u_1-u_0,$$

ce qui prouve que notre propriété est vraie au rang $n=0$.

- **Hérédité :** Soit $n\in\mathbb{N}$. Supposons que la propriété est vraie pour ce n, c'est à dire que

$$\sum_{k=0}^{n}(u_{k+1}-u_k)=u_{n+1}-u_0.$$

Dans ce cas, au rang $n+1$ on a

$$\begin{aligned}S_{n+1}&=\sum_{k=0}^{n+1}(u_{k+1}-u_k)\\&=\sum_{k=0}^{n}(u_{k+1}-u_k)+(u_{n+2}-u_{n+1})\\&\underset{HR}{=}(u_{n+1}-u_0)+(u_{n+2}-u_{n+1})\\&=u_{n+2}-u_0.\end{aligned}$$

Ce qui achève notre récurrence.

Le résultat sur la somme des nombres entiers impairs en découle en considérant la suite (u_n) définie par $u_n=n^2$.

Exemple 2 Nous nous intéressons dans ce deuxième exemple à une somme similaire définie par

$$\begin{aligned}S_1&=1=1^2\\S_2&=1+2+1=4=2^2\\S_3&=1+2+3+2+1=9=3^2\\S_4&=1+2+3+4+3+2+1=16=4^2\\&\vdots\\S_n&=1+2+3+\cdots+(n-1)+n+(n-1)+(n-2)+\cdots+1\underset{?}{=}n^2.\end{aligned}$$

Notre conjecture semble vraie et c'est une application directe du principe de la récurrence.

En effet

- **Initialisation :** Comme nous venons de voir, la propriété est vraie pour $n = 1$.
- **Hérédité :** Soit $n \geq 1$. Supposons que la propriété est vraie pour ce n, à savoir que

$$S_n = 1+2+3+\cdots(n-1)+n+(n-1)+(n-2)+\cdots+1 = n^2.$$

La somme S_{n+1} s'obtient à partir de S_n en additionnant les entiers $n+1$ et n. Ainsi on a

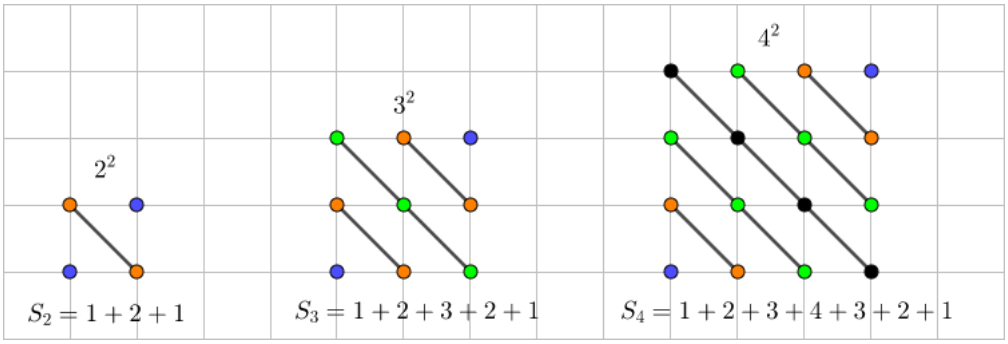
$$\begin{aligned} S_{n+1} &= S_n + (n+1) + n \\ &= n^2 + 2n + 1 \\ &= (n+1)^2. \end{aligned}$$

Ceci achève notre récurrence.

Remarquez qu'on aurait pu se passer de ce raisonnement en procédant directement de la façon suivante

$$\begin{aligned} S_n &= \underbrace{1+2+3+\cdots+(n-1)+n}_{\frac{n(n+1)}{2}} + \underbrace{(n-1)+(n-2)+\cdots+1}_{\frac{n(n-1)}{2}} \\ &= \frac{n(n+1)}{2} + \frac{n(n-1)}{2} \\ &= \frac{n(n+1+n-1)}{2} \\ &= n^2 \end{aligned}$$

Ici encore, une visualisation géométrique vaut bien mieux qu'une preuve formelle. Voilà ce qui se passe avec un petit dessin



Il est temps maintenant de se poser une question fondamentale : peut-on se passer de l'initialisation dans un raisonnement par récurrence ? La réponse est non comme le montre le contre-exemple ci-dessous.

Soit $\mathscr{P}(n)$ la propriété " 3 divise 4^n ". Nous allons démontrer la validité de l'hérédité, c'est à dire que si $\mathscr{P}(n)$ est vraie alors $\mathscr{P}(n+1)$ l'est aussi. Pourtant la propriété $\mathscr{P}(n)$ ne sera vraie pour aucun entier naturel n. Il n'y aura aucun rang pour lequel on pourra initialiser notre propriété et notre file infinie de dominos ne tombera pas.

- **Hérédité** Soit $n \in \mathbb{N}$ et supposons que pour ce n fixé 3 divise 4^n. Il existe alors un entier k pour lequel $4^n = 3k$. Cela implique que

$$4^{n+1} = 4 \times 4^n = 4 \times 3k = 3 \times 4k,$$

ce qui implique que 3 divise 4^{n+1}. Toutefois, à aucun endroit 3 divise 4^n, puisque 3 est un nombre premier et le seul nombre premier divisant 4^n est 2. Par unicité de la décomposition d'un entier naturel en facteurs premiers, 3 ne peut donc pas figurer dans celle-ci. Par ailleurs, pour ceux qui connaissent les congruences, le reste de la division euclidienne de 4 par 3 vaut 1. Cela s'écrit $4 \equiv 1 \pmod 3$, on peut alors voir le signe $\equiv$ comme une égalité dans un autre monde de nombres, une égalité qui se comporte bien par rapport au passage à une puissance n. Ainsi $4 \equiv 1 \pmod 3$ implique que $4^n \equiv 1^n \pmod 3 \equiv 1 \pmod 3$. Du coup, le reste de la division euclidienne de 4^n par 3 vaut toujours $1 \neq 0$. Pour s'en convaincre, les premières puissances de 4 donnent

$$\begin{aligned} 4^2 &= 16 = 3 \times 5 + 1 \\ 4^3 &= 64 = 3 \times 21 + 1 \\ 4^4 &= 256 = 3 \times 85 + 1 \\ &\vdots \end{aligned}$$

Moralité, il faut toujours initialiser la récurrence sinon cela risque de ne pas fonctionner.

Nous terminons cette section avec un paradoxe dû au logicien Alfred Tarski.

Alfred Tarski

Soit $\mathscr{P}(n)$ la propriété

Dans toute collection de n nombres $a_1, a_2, \ldots, a_n$, ces nombres sont tous égaux.

Autrement dit $a_1 = a_2 = \cdots = a_n$. Le moins qu'on puisse dire sur cet énoncé c'est qu'il est très FAUX. Pour $n = 3$, si $a_1 = 2, a_2 = 5$ et $a_3 = 7$, rien ne peut affirmer que $a_1 = a_2 = a_3$ et puis c'est erroné. Toutefois, nous allons bien démontrer l'énoncé de Tarski par récurrence. En effet

- **Initialisation :** Si $n = 1$, il n'y a qu'un nombre, à savoir a_1 et on a bien $a_1 = a_1$. L'énoncé est donc vrai.

- **Hérédité :** Soit $n \geq 1$. Supposons que la propriété est vraie pour ce n et montrons que cela implique $\mathscr{P}(n+1)$. Soit donc $a_1, a_2, \ldots a_{n+1}$ une collection contenant $n+1$ nombres. La collection $a_1, a_2, \ldots, a_n$ est une collection contenant n nombres donc l'hypothèse de la récurrence implique que $a_1 = a_2 = \cdots = a_n$. De même, la collection $a_2, a_3, \ldots, a_{n+1}$ est une collection de n nombres donc sont tous égaux, à savoir $a_2 = a_3 = \cdots = a_{n+1}$. Cela implique donc que

  $$a_1 = a_2 = a_3 = \cdots = a_n = a_{n+1}.$$

  Ceci achève donc notre récurrence ! ! ! Ce résultat intuitivement faux serait-il réellement démontrable par récurrence ? Cela remet-il en cause notre fameux principe ? Où se trouve l'erreur dans ce raisonnement. Je vous invite à méditer avant de lire la suite.

Le passage de $n = 2$ à $n = 3$ ne pose aucun problème. De même le passage de $n = 3$ à $n = 4$ et tous les autres passages de n à $n+1$ se passent sans histoires. Toutefois, le passage de $n = 1$, c'est à dire notre initialisation, à $n = 2$ est impossible. Toute la récurrence tombe donc à l'eau.

5 Le principe de la descente infinie de Fermat

Nous inspectons dans ce paragraphe le fameux principe de la descente infinie de Fermat. Bien qu'il ne soit pas enseigné dans le parcours scolaire ordinaire, nous verrons ensemble qu'il est d'une importance capitale en arithmétique. Ce principe, comme son nom l'indique, a été inventé par notre éminent ancêtre *Pierre de Fermat* afin de répondre à des questions de la théorie des nombres.

Pierre de Fermat

Ce principe affirme tout simplement qu'on ne peut pas construire une suite strictement décroissante d'entiers naturels. J'espère que cela semble évident pour vous car en effet si (u_n) est une suite d'entiers naturels alors pour tout $n \in \mathbb{N}, u_n \geq 0$. De plus si par exemple $u_0 = 12$ alors u_1 doit être un entier naturel strictement plus petit que u_0, prenons $u_1 = 9$. De même, $u_2 < u_1$ et $u_3 < u_2$ etc. On voit donc que cette suite ne peut pas descendre infiniment car elle doit rester positive. Plus formellement, l'ensemble

$$U = \{u_n, n \in \mathbb{N}\} \subset \mathbb{N}$$

est un sous-ensemble non vide de $\mathbb{N}$, il admet ainsi un plus petit élément u_{n_0} [6]. Or la suite (u_n) est strictement décroissante, par conséquent $u_{n_0+1} < u_{n_0}$. Cela signifie que u_{n_0+1} est un élément de U plus petit que son plus petit élément u_{n_0}. Cela conduit évidemment à une *contradiction*. Ainsi pour démontrer l'impossibilité d'un énoncé arithmétique, il suffit de construire à partir de celui-ci une suite strictement décroissante d'entiers naturels. Un exemple vaut mieux qu'un long discours.

Exemple1 : Dans cet exemple, nous allons démontrer que $\sqrt{2}$ est un nombre irrationnel. Autrement dit $\sqrt{2}$ ne peut pas s'écrire sous la forme d'une fraction p/q. Pour se faire, supposons qu'il existe un couple (p,q) d'entiers naturels tel que

$$\sqrt{2} = \frac{p}{q} \quad \text{où } p > q.$$

Cela implique en élévant au carré que $2 = p^2/q^2$ ou encore que $p^2 = 2q^2$. Par conséquent p^2 est un nombre pair et donc p l'est aussi [7]. Notre entier p s'écrit donc sous la forme $p = 2k$, où k désigne un entier naturel. La relation $p^2 = 2q^2$ implique alors la relation $(2k)^2 = 2q^2$ ou encore

$$2k^2 = q^2.$$

Cette relation s'écrit $\sqrt{2} = q/k$ où $q > k$, auquel cas on obtient une deuxième représentation de $\sqrt{2}$ sous forme d'une fraction. Notez alors qu'on a construit les trois premiers termes d'une suite d'entiers naturels tels que $p > q > k$. Nous pouvons construire de même un nouvel entier naturel x tel que $\sqrt{2} = k/x$ et $p > q > k > x$. En réitérant ce même procédé, nous pouvons construire une suite strictement décroissante d'entiers naturels. Cela conduit donc à une contradiction d'après le principe de la descente infinie de Fermat. D'où l'irrationalité de $\sqrt{2}$. Dans le monde mathématique, il existe plusieurs preuves de l'irrationalité de $\sqrt{2}$. L'une d'elle est une preuve géométrique (celle que je préfère à titre personnel), bien plus parlante que la preuve utilisant des arguments arithmétiques. Nous n'aborderons pas cette preuve ici mais notez qu'elle fournit une autre suite strictement décroissante d'entiers naturels prouvant là encore l'irrationalité de $\sqrt{2}$. En effet, l'identité qui découle de l'argument géométrique est

$$\sqrt{2}(\sqrt{2}-1) = 2-\sqrt{2}.$$

Cette identité s'écrit aussi sous la forme

$$\sqrt{2} = \frac{2-\sqrt{2}}{\sqrt{2}-1}.$$

Ainsi si $\sqrt{2} = p/q$ alors on obtient

$$\sqrt{2} = \frac{p}{q} = \frac{2-\frac{p}{q}}{\frac{p}{q}-1} = \frac{2q-p}{p-q}.$$

Aha, pas mal tout ça ! Je viens de trouver une nouvelle fraction égale à $\sqrt{2}$. Il nous reste à démontrer que $q > p-q$. Autrement dit, le dénominateur de la première fraction est strictement plus grand que le dénominateur de la deuxième. Cette inégalité est relativement

6. Par l'axiome du bon ordre qui dit que tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément.

7. Nous pouvons démontrer aisément que si p^2 est un entier pair alors p est pair aussi. En effet, si p est impair alors il s'écrit sous la forme $p = 2k+1$, son carré s'écrit alors $p^2 = 2(2k^2+2k)+1$, qui est un nombre impair. Autrement dit si p^2 est pair, p ne peut pas être impair car son carré serait impair !

triviale puisqu'elle est équivalente à l'inégalité $2 > p/q = \sqrt{2}$. Par ailleurs le dénominateur $p-q$ de notre nouvelle fraction est bien un entier positif car rappelez-vous $p > q$. L'irrationalité de $\sqrt{2}$ découle alors de l'impossibilité de la construction d'une telle suite. Merci Fermat !

Exemple2 : Nous nous intéressons dans ce deuxième exemple à un énoncé qui a fait couler beaucoup d'encre. Nous avons vu ensemble que l'équation $x^2 + y^2 = z^2$ admet une infinité de solutions, à savoir les triplets pythagoriciens. Notre regretté Fermat s'est alors posé la question naturelle, à savoir l'équation $x^3 + y^3 = z^3$ admet-elle des solutions entières telles que $xyz \neq 0$ [8] ? Plus généralement, si $n \geq 3$ et $xyz \neq 0$, peut-on résoudre l'équation $x^n + y^n = z^n$ chez les entiers ? Cette dernière question s'appelle le Grand Théorème de Fermat, Fermat lui-même prétend avoir trouvé une preuve à l'impossibilité de la résolution d'une telle équation. Toutefois, il ne publie rien et dit que la marge est trop petite pour qu'il puisse y mettre sa démonstration. Cette conjecture n'a été démontré que par son éminence, le mathématicien britannique Andrew Wiles en 1995, c'est à dire environ 350 années après Fermat, en utilisant au passage un arsenal technique extrêmement sophistiqué, dépassant de bien loin le cadre de notre cours !

Andrew Wiles

Fermat a su toutefois démontrer sa conjecture pour $n = 4$, à savoir si $xyz \neq 0$, l'équation $x^4 + y^4 = z^4$ n'admet pas de solutions. Dans notre cas, nous esquisserons [9] sa preuve. L'une des manières pour démontrer qu'un énoncé est impossible est de lui trouver une conséquence impossible. Mais quelle conséquence donc pour notre petit énoncé ? ! Fermat établit en effet un lien avec les triangles pythagoriciens, à savoir les triangles rectangles dont les côtés sont des entiers. Il démontre que

si $x^4 + y^4 = z^4$ était résoluble dans nos conditions alors il pourrait construire un triangle pythagoricien ayant une aire un carré parfait !

Notre ancêtre démontre alors avec son principe de la descente infinie que ce dernier résultat est impossible : il n'existe pas de triangle pythagoricien dont l'aire est un carré parfait. Pour se faire, il démontre que si un tel triangle existe, alors on pourra construire un triangle strictement plus petit ayant la même propriété. Ici, nous expliciterons seulement le lien en

8. Le cas $xyz = 0$ est trivial et est laissé au lecteur.
9. Nous manquerons d'outils pour l'instant pour finaliser cette démonstration mais nous y reviendrons plus loin.

rouge. En effet, nous avons vu que les triplets pythagoriciens sont tous de la forme $(u^2 - v^2, 2uv, u^2 + v^2)$. Ainsi, si x, y et z vérifie l'équation $x^4 + y^4 = z^4$ alors $x^4 = z^4 - y^4$, ce qui implique que le triplet

$$(z^4 - y^4, 2z^2y^2, z^4 + y^4)$$

est un triplet pythagoricien. L'aire de ce triangle vaut alors

$$\frac{1}{2}(z^4 - y^4) \times 2z^2y^2 = x^4z^2y^2 = (x^2zy)^2.$$

On obtient ainsi un triangle pythagoricien dont l'aire est un carré parfait. Contradiction. Très ingénieux, cela demande de la technique et Fermat n'en manquait pas ! Nous terminerons cette preuve quand on disposera de suffisamment d'artillerie arithmétique.

6 L'axiome du bon ordre et le principe de la récurrence

Ce paragraphe est une petite digression légèrement futuriste. En effet, nous avons parlé rapidement de l'axiome du bon ordre, à savoir tout sous-ensemble non vide de $\mathbb{N}$ admet un plus petit élément. Ce résultat nous parait intuitivement évident. Bien sûr, si on prend un ensemble constitué d'entiers naturels alors il existe un plus petit entier parmi ceux-là. Mais rien n'est bien évident trop longtemps en mathématiques. On pourrait très bien se dire comment sont contruits les entiers naturels à la base ? Et puis qu'est ce qui garantit leur consistence ? Peut-on autrement dit tomber un jour sur un paradoxe chez les entiers ? Cela serait peut être une catastrophe mathématique, tout tombera à l'eau !

Dans notre cas en tout cas, si on accepte le principe de la récurrence, on pourra démontrer relativement sans beaucoup de travail l'axiome du bon ordre. En effet, on pourra démontrer de façon équivalente que si A est une partie de $\mathbb{N}$ sans petit élément alors A est vide. Pour se faire, on montre par récurrence la propriété $\mathscr{P}(n)$

$$\text{pour tout } i \leq n,\ i \notin \text{A}.$$

- **Initialisation :** $\mathscr{P}(0)$ est vraie car sinon 0 serait le plus petit élément de A.
- **Hérédité :** Soit $n \in \mathbb{N}$. Supposons que $\mathscr{P}(n)$ est vraie. On sait alors que pour tout $i \leq n$, $i \notin$ A. Par ailleurs, puisque A n'admet pas de plus petit élément, elle ne peut pas contenir $n+1$ (car sinon $n+1$ serait le plus petit élément de A). Ainsi on a démontré que

  $$\text{pour tout } i \leq n+1\ ,\ i \notin \text{A}.$$

  D'où $\mathscr{P}(n+1)$. Élégant n'est ce pas ? !

En vrai (et c'est incroyable), l'axiome du bon ordre implique le principe de la récurrence ! ! ! En plus clair, si on accepte l'axiome du bon ordre comme intuitivement évident alors on pourra démontrer le principe de la récurrence. En effet, soit $\mathscr{P}$ une propriété vérifiant les conditions de la récurrence, c'est à dire que

1. $\mathscr{P}(0)$ est vraie.
2. Pour tout $n \in \mathbb{N}$, si $\mathscr{P}(n)$ est vraie alors $\mathscr{P}(n+1)$ l'est aussi.

Supposons par l'absurde que $\mathscr{P}$ est fausse pour quelques entiers naturels. Soit A la partie

$$\{n \in \mathbb{N} / \mathscr{P}(n) \text{ est fausse}\}.$$

Par hypothèse, A est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément d'après l'axiome du bon ordre. On notera cet élément n_0. D'après l'hypothèse de la récurrence $n_0 \neq 0$ car $\mathscr{P}(0)$ est vraie. On pourra donc considérer l'entier naturel $n_0 - 1$ pour lequel la propriété $\mathscr{P}$ est vraie (car n_0 est le plus petit pour lequel la propriété $\mathscr{P}$ est fausse). Encore d'après l'hypothèse de la récurrence

$$\mathscr{P}(n_0 - 1) \implies \mathscr{P}(n_0).$$

Cela implique du coup que $\mathscr{P}(n_0)$ est vraie. Contradiction, la partie A est ainsi vide et $\mathscr{P}(n)$ est vraie pour tout n. Trop philosophique pour vous ? Vous apprécierez ce paragraphe plus tard dans nos aventures mathématiques.

7 Une première rencontre avec les nombres premiers

Vous n'êtes pas sans savoir (je l'espère) que les nombres premiers sont les éléments de base permettant la construction de tous les entiers naturels > 1 par multiplication. Ainsi, tout entier $n \geq 2$ est le produit de nombres premiers (pas nécéssairement distincts) mais un nombre premier ne s'obtient qu'en le multipliant par 1. On obtient donc la définition suivante

Définition : Un nombre premier est un entier naturel admettant exactement deux diviseurs, 1 et lui-même.

Cette définition implique que 1 n'est pas un nombre premier car certes celui-ci est divisible par 1 et par lui-même mais il ne s'agit que d'un seul diviseur ($1 =$ lui-même) alors que dans notre définition on demande exactement deux diviseurs. Une définition équivalente consiste à dire qu'un nombre premier est un entier naturel $p \neq 1$ divisible uniquement par 1 et par lui-même. Remarquez qu'ici on exclut 1 dès le départ car 1 vérifie la deuxième condition "être divisible uniquement par 1 et par lui-même". Beaucoup se posent la question du pourquoi exclure l'entier 1 de l'ensemble des nombres premiers ! Eh bien, en théorie des nombres, on considère qu'une bonne arithmétique est celle dans laquelle il y a unicité de la factorisation en éléments premiers ! L'entier 1 fait défaut à cette histoire et d'autres aussi, d'où son exclusion. Vous comprendrez cette remarque plus en profondeur si vous vous décidez de vous plonger davantage dans la théorie des nombres.

On voit alors que $p_1 = 2$ est le premier nombre premier (et le seul pair, pourquoi ?) car divisible uniquement par 1 et par lui-même. Le nombre $p_2 = 3$ est le deuxième nombre premier de la liste des nombres premiers, 4 n'est pas premier car il est divisible par 2 qui n'est ni 1 ni lui-même etc. Notez alors que la définition des nombres premiers semble d'une grande facilité, toutefois ces nombres nous donnent beaucoup de mal car sont de nature très profonde et très difficile à décortiquer. La théorie des nombres se caractérise par la facilité de l'énoncé de beaucoup de ses problèmes, qui demeurent toutefois très difficiles à résoudre ou même qui dépassent de bien loin les connaissances (très sophistiquées) actuelles en mathématiques. Citons à titre d'exemple la fameuse conjecture de **Goldbach** : tout entier naturel pair plus grand ou égal à 4 peut s'écrire comme la somme de deux nombres premiers. En essayant les premières valeurs on obtient le tableau suivant

n	Décomposition
4	$2+2$
6	$3+3$
8	$5+3$
10	$7+3$
12	$7+5$
$\vdots$	$\vdots$

Je vous invite à inspecter davantage d'entiers naturels pairs pour se rendre compte de la plausibilité de cette conjecture.

Les nombres premiers sont bien rares parmi les nombres entiers dès qu'on s'intéresse à des nombres bien grands. Cela s'explique grosso modo par le fait qu'un grand nombre a potentiellement plus de diviseurs qu'un petit nombre. Toutefois, malgré leur rareté, Euclide a réussi à démontrer dans son *Livre 9* des *Éléments* qu'il en existe une infinité.

Euclide : Il existe une infinité de nombres premiers.

Avant de vous présenter la preuve (très élégante) d'Euclide, nous démontrons que tout nombre entier $n \geq 2$ est le produit de nombres premiers (pas forcément distincts). Cela impliquera en particulier que tout nombre entier $n \geq 2$ admet au moins un diviseur premier. Cette dernière affirmation nous sera utile dans la démonstration d'Euclide. Pour se faire, nous procéderons de deux manières, la première utilisant l'axiome du bon ordre et la deuxième le principe de la récurrence.

1. **Le bon ordre :** Supposons par l'absurde qu'il existe des entiers naturels > 1 qui ne soient pas produits de nombres premiers. D'après l'axiome du bon ordre l'ensemble de ces nombres admet un plus petit élément z. Cet entier n'est pas premier car sinon on pourrait écrire $z = z$ (il s'agit du produit d'un seul élément premier). Donc z est un nombre composé et s'écrit sous la forme $z = xy$, où $1 < x < z$ et $1 < y < z$. Par minimalité de z, les entiers x et y sont produits d'éléments premiers et s'écrivent donc sous la forme
$$x = p_1 p_2 \cdots p_r \quad \text{et} \quad y = q_1 q_2 \cdots q_t$$
où $p_1, p_2, \ldots p_r$ et $q_1, q_2, \ldots q_t$ sont des nombres premiers. Par conséquent
$$z = xy = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_t$$
est produit de nombres premiers. Contradiction ! Le résultat en découle.

2. **La récurrence :** Soit $\mathscr{P}(n)$ la propriété

   tout entier > 1 et $\leq n$ est produit de nombres premiers.

   - **Initialisation :** La propriété est triviale pour $n = 2$ car comme 2 est premier, il est le produit d'un seul nombre premier, à savoir lui-même.
   - **Hérédité :** Soit $n \geq 2$ et supposons que $\mathscr{P}(n)$ est vraie. Si $n+1$ est premier alors cela coule de source. Sinon, $n+1$ est un nombre composé et s'écrit donc sous la forme $n+1 = xy$ où $1 < x \leq n$ et $1 < y \leq n$. Ainsi d'après l'hypothèse de la récurrence x et y sont produits de nombres premiers et donc leur produit $n+1$ l'est aussi. Ceci achève donc notre brave petite récurrence.

Passons maintenant à la belle démonstration d'Euclide. Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers qu'on note $p_1, p_2, \ldots, p_n$. Soit N le nombre

$$N = p_1 p_2 \cdots p_n + 1.$$

D'après ce qui précède, $N > 1$ admet au moins un diviseur premier p. Je prétends alors que p est distinct de $p_1, p_2, \ldots, p_n$, ce qui conduira à une contradiction car on a supposé que $p_1, p_2, \ldots, p_n$ sont les seuls nombres premiers. En effet, si p était l'un des p_i il diviserait leur produit $p_1 p_2 \cdots p_n$. Par ailleurs, p divise N donc doit diviser la différence $N - p_1 p_2 \cdots p_n = 1$. Le nombre premier p divise donc 1, ce qui n'est pas. Cette contradiction implique donc qu'il existe une infinité de nombres premiers.

Tâchons maintenant de voir ce qui se passe expérimentalement avec la preuve euclidienne. On aimerait en effet évaluer le nombre N avec les premiers nombres premiers, d'où le tableau suivant.

N
$p_1 + 1 = 2 + 1 = 3$
$p_1 \cdot p_2 + 1 = 2 \times 3 + 1 = 7$
$p_1 \cdot p_2 \cdot p_3 + 1 = 2 \times 3 \times 5 + 1 = 31$
$p_1 \cdot p_2 \cdot p_3 \cdot p_4 + 1 = 2 \times 3 \times 5 \times 7 + 1 = 211$
$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 + 1 = 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$
$\vdots$

On voit alors que les premiers nombres N générés par la formule d'Euclide sont premiers. Toutefois, la preuve d'Euclide dit tout simplement que N admet un diviseur premier. Euclide avait raison de ne pas considérer N comme premier car par exemple le nombre

$$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot p_6 + 1 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 59 \times 509$$

n'est pas premier. De même, si on va un peu plus loin, le nombre

$$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot p_6 \cdot p_7 + 1 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 + 1 = 19 \times 97 \times 277$$

n'est pas premier non plus. Trop beau pour être vrai. Bien que l'on sache qu'il en existe une infinité, il est très difficile de trouver des nombres premiers très grands. La quête des nombres premiers se poursuit toujours, non seulement parce qu'il s'agit d'un moyen de mesurer la puissance de nos ordinateurs mais aussi parce qu'ils sont très utiles en cryptographie. Avant de conclure ce paragraphe, notez le tour de force technique et psychologique dans la preuve d'Euclide. En effet, ce dernier prouve l'existence d'un nombre infini d'objets sans pouvoir tous les exhiber, ce qui était révolutionnaire pour son époque. D'où son élégance.

La formule d'Euclide ne produit pas que des nombres premiers et la question toute naturelle est : existe-t-il une formule générale relativement simple permettant de générer les nombres premiers ? L'expérimentation montre que l'existence d'une telle formule magique est très peu probable car on ne peut pas prédire la position des nombres premiers parmi les entiers naturels. S'il existe une formule simple générant le n—ième nombre premier p_n alors il existerait une formule simple permettant de trouver la différence entre deux nombres premiers consécutifs $p_{n+1} - p_n$. L'expérimentation là encore montre que cette différence est

extrêmement irrégulière et l'on peut la rendre aussi grande que l'on veut. En effet, pour tout entier $n \geq 2$, les $n-1$ nombres consécutifs

$$n!+2, \quad n!+3, \quad n!+4\ldots, \quad n!+n \quad \text{où } n! = 1\times 2\times 3\cdots\times n$$

sont tous composés (le premier est divisible par 2, le deuxième par 3 etc). Si on prend par exemple $n = 10000$ alors cette suite de nombres fournit 9999 nombres entiers consécutifs dont aucun n'est premier.

Malgré l'extrême difficulté de cette quête, nous n'allons tout de même pas l'abandonner à mi-chemin. Nous pouvons explorer de nouvelles idées et voir si cela permet d'aboutir à davantage de compréhension de nos supers nombres. Soit $\mathbb{P} = \{p_1, p_2, \ldots, p_n, \ldots\}$ la liste des nombres premiers et soit p [10]le nombre défini par

$$p = \sum_{k=1}^{+\infty} \frac{1}{10^{p_k}} = \frac{1}{10^{p_1}} + \frac{1}{10^{p_2}} + \cdots \frac{1}{10^{p_n}} + \cdots$$

Je vois que vous commencez à avoir peur. C'est tout à fait naturel mais il n'y a rien de bien compliqué dans cette somme. En effet, on a

$$\begin{aligned} p &= \sum_{k=1}^{+\infty} \frac{1}{10^{p_k}} \\ &= \frac{1}{10^{p_1}} + \frac{1}{10^{p_2}} + \cdots \frac{1}{10^{p_n}} + \cdots \\ &= \frac{1}{10^2} + \frac{1}{10^3} + \frac{1}{10^5} + \frac{1}{10^7} + \frac{1}{10^{11}} + \cdots \\ &= 0.01 + 0.001 + 0.00001 + 0.0000001 + 0.00000000001 + \cdots \\ &= 0.0110101000101000101\cdots \end{aligned}$$

On remarque alors que le développement décimal du nombre p indique la position des nombres premiers. En effet, sa première décimale vaut 0 ce qui signifie que 1 n'est pas premier, sa deuxième décimale vaut 1 indiquant que 2 est premier, sa troisième décimale vaut 1 aussi indiquant que 3 est premier, sa 4ème décimale vaut 0 ce qui signifie que 4 est un nombre composé etc. Notez alors que pour calculer notre nombre p, nous avons d'abord besoin de connaître les nombres premiers. Si on trouve un jour un autre moyen permettant de le calculer sans les nombres premiers, on gagnera au loto ! Mais pour l'instant, rien n'est gagné !

En 1640, Fermat a écrit à Mersenne autour d'une fameuse formule qui ne produit que des nombres premiers, à savoir la suite (F_n) définie pour tout $n \in \mathbb{N}$ par

$$F_n = 2^{2^n} + 1.$$

10. Pour les fous de l'analyse, ce nombre existe bien car la série de terme général $\frac{1}{10^{p_n}}$ est convergente. En effet, tous les termes de cette série sont positifs donc

$$\sum_{k=1}^{+\infty} \frac{1}{10^{p_k}} \leq \sum_{k=1}^{+\infty} \frac{1}{10^k} = \frac{1}{9}$$

Marin Mersenne

Malgré son génie, Fermat a pensé et à tort que les F_n sont tous premiers. Après une petite expérimentation, on obtient le tableau suivant

n	F_n
0	$2^{2^0}+1=3$
1	$2^{2^1}+1=5$
2	$2^{2^2}+1=17$
3	$2^{2^3}+1=257$
4	$2^{2^4}+1=65537$
$\vdots$	$\vdots$

Vous pouvez alors vérifier que les 5 premiers nombres F_n sont tous premiers, toutefois, Euler a prouvé avec une méthode ingénieuse que le nombre

$$F_5 = 2^{2^5}+1 = 2^{32}+1$$

est un multiple de 641. Pour reproduire cette preuve, nous utiliserons les congruences et il suffit de savoir pour la comprendre que le signe " $\equiv$ " se comporte grosso modo comme le signe " $=$ " (*) et que pour montrer que F_5 est divisible par 641 il suffit de montrer que

$$F_5 \equiv 0 \pmod{641}.$$

Ce résultat est équivalent à montrer que $2^{32}+1 \equiv 0 \pmod{641}$, ou encore à $2^{32} \equiv -1 \pmod{641}$ (par la remarque *). Pour se faire, d'abord on sait que $641 \equiv 0 \pmod{641}$ (car 641 divise 641). Puisque $641 = 640+1 = 5\times 2^7+1$, cela implique en particulier que

$$5\times 2^7+1 \equiv 0 \pmod{641},$$

ou encore que $5\times 2^7 \equiv -1 \pmod{641}$. De même par la remarque * on pourra élever cette "égalité" à la puissance 4 pour obtenir

$$5^4\times 2^{28} \equiv (-1)^4 \pmod{641} \equiv 1 \pmod{641}. \tag{1}$$

Par ailleurs l'égalité $641 = 625 + 16 = 5^4 + 2^4$ implique aussi que $5^4 + 2^4 \equiv 0 \pmod{641}$ ou encore que $5^4 \equiv -2^4 \pmod{641}$. Ainsi en remplaçant 5^4 par -2^4 dans la congruence (1) on obtient

$$-2^4 \times 2^{28} \equiv 1 \pmod{641},$$

ou encore $2^{32} \equiv -1 \pmod{641}$. Le résultat en découle et la question toute naturelle est d'où sort 641 à la base ? Est-ce le génie d'Euler ou alors une recette secrète utilisée par notre ancêtre ? Nous répondrons à cette question au bon moment ! Cette preuve semble un peu technique pour l'instant mais ce n'en est rien. Nous verrons que tout deviendra trivial quand on étudiera en détail les *congruences*. Depuis le temps d'Euler, les mathématiciens ont su démontrer que d'autres nombres de Fermat sont composés et l'on pourra vérifier que $F_6 = 2^{64} + 1$ est divisible par 274177. Notez alors que personne n'a trouvé encore un nombre de Fermat premier pour $n \geq 5$.

Dans la suite de cette section, nous donnons une deuxième preuve de l'infinité des nombres premiers utilisant les nombres de Fermat. Cette idée géniale est due au grand mathématicien hongrois George Pólya.

George Pólya

Pour se faire nous allons démontrer que les nombres de Fermats sont deux à deux premiers entre eux, ce qui signifie qu'ils n'ont aucun diviseur en commun plus grand que 1. Nous pouvons observer en effet l'identité suivante

$$F_0 F_1 F_2 \cdots F_n = F_{n+1} - 2.$$

Pas très évident tout ça allez-vous me dire ! En multipliant le membre de gauche de cette égalité par $2^{2^0} - 1 = 1$ on obtient

$$\begin{aligned}
\left(2^{2^0} - 1\right) F_0 F_1 F_2 \cdots F_n &= \left(2^{2^0} - 1\right)\left(2^{2^0} + 1\right) F_1 F_2 \cdots F_n \\
&= \left(\left(2^{2^0}\right)^2 - 1^2\right) F_1 F_2 \cdots F_n \\
&= \left(2^{2^1} - 1\right)\left(2^{2^1} + 1\right) F_2 \cdots F_n \\
&= \left(\left(2^{2^1}\right)^2 - 1^2\right) F_2 \cdots F_n \\
&\vdots \\
&= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) \\
&= 2^{2^{n+1}} - 1 \\
&= 2^{2^{n+1}} + 1 - 2 \\
&= F_{n+1} - 2.
\end{aligned}$$

J'avoue que c'est bien astucieux mais cette astuce est fort connue depuis le temps d'Euler, pour qui il s'agit d'une trivialité comparée à ses capacités algébriques. Je vous rappelle alors qu'on a établi cette identité afin de prouver que les nombres de Fermat sont deux à deux premiers entre eux. Soient en effet F_n et F_m deux nombres de Fermat tels que $m < n$ et soit d un diviseur positif en commun à F_n et F_m. On souhaite démontrer que $d = 1$. L'entier d doit diviser alors

$$F_n - (F_0 \cdots F_m \cdots F_{n-1}) = 2.$$

Ceci implique en particulier que $d \in \{1, 2\}$, d ne peut pas être égal à 2 car les F_n sont des nombres impairs. Le résultat en découle. Maintenant pour montrer qu'il existe une infinité de nombres premiers, il suffit de remarquer que chacun des F_n doit admettre au moins un diviseur premier et ce diviseur ne divise aucun des autres nombres de Fermat. Puisque les nombres de Fermat sont en nombre infini, les nombres premiers le sont aussi. Ingénieux, n'est ce pas ?

8 Le théorème de la division euclidienne

Avant d'aller plus loin, nous devons tout de même toucher un mot sur le théorème de la division euclidienne sur lequel repose toute l'arithmétique. Ce théorème (lui aussi intuitivement évident) est fort connu du grand public, puisqu'on l'a tous étudier à l'école primaire : il s'agit en effet de la division avec un quotient et un reste. Prenons donc quelques exemples afin de le bien cerner.

Exemple 1 : Le nombre 42 n'est pas divisible par 11. En effet,

$$11 \cdot 0 = 0, \quad 11 \cdot 1 = 11, \quad 11 \cdot 2 = 22, \quad 11 \cdot 3 = 33, \quad 11 \cdot 4 = 44.$$

On voit ainsi qu'il n'existe pas d'entier n tel que $11n = 42$. Le plus grand multiple de 11 en dessous de 42 est 33 et il reste donc 9 pour arriver à 42. Autrement dit $42 - 11 \cdot 3 = 9$ ou encore

$$42 = 11 \cdot 3 + 9.$$

Remarquez alors que 9 est plus petit entier positif parmi les entiers de la forme $42 - 11n$ et que $0 \leq 9 < 11$. Notez aussi que $q = 3$ est le seul entier tel que $42 - 11q = 9$ et qu'il n'existe pas d'autre entier $n \in \mathbb{Z}$ avec $r = 42 - 11n$ et $0 \leq r < 9$, puisque 9 est le plus petit entier vérifiant ces dernières inégalités.

Exemple 2 : Le nombre 57 n'est pas multiple de 13. Quel est donc le reste de la division euclidienne de 57 par 13 ? Pour répondre à cette question, on calcule mentalement le plus grand multiple de 13 en dessous de 57, qui est dans notre cas $13 \cdot 4 = 52$. Ainsi, le reste de la division euclidienne de 57 par 13 vaut $57 - 13 \cdot 4 = 5$. On écrit donc

$$57 = 13 \cdot 4 + 5.$$

Notez alors que pour trouver ce reste, on a parcouru mentalement tous les nombres r de la forme $r = 57 - 13 \cdot n$ jusqu'à ce qu'on tombe sur un r vérifiant les inégalités $0 \leq r < 13$, puisqu'ici on divise par 13.

Nous sommes maintenant prêt à énoncer le brave théorème de la division euclidienne et à le démontrer en généralisant les deux exemples précédents.

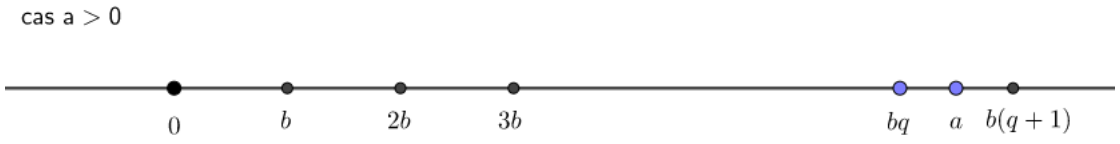
Théorème : Soient a et b deux entiers tels que $b > 0$. Il existe un unique couple (q, r) dans $\mathbb{Z}^2$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

- Montrons d'abord l'existence de q et r. Considérons l'ensemble

$$A = \{a - bm \geq 0 \mid m \in \mathbb{Z}\}$$

A est un sous-ensemble non vide de $\mathbb{N}$. En effet, si $a \geq 0$, il contient $a - b \times 0$. Sinon, il contient $a - ba$. Ainsi, d'après l'axiome du bon ordre il contient un plus petit élément. Appelons cet élément r. L'entier r vérifie alors l'égalité $r = a - bq$ pour un certain $q \in \mathbb{Z}$, par définition de A. De même, $r \geq 0$ par définition. Par ailleurs, $r < b$ car si $r \geq b$, alors $a - b(q+1) \in A$, ce qui est en contradiction avec le fait que r soit le plus petit élément de A.



- Montrons maintenant que (q, r) est unique. Soit (q', r') un deuxième couple de la division euclidienne de a par b. Alors $|r' - r| < b$ [11] et l'égalité $bq + r = bq' + r'$ implique que $b(q - q') = r' - r$. Au final, on obtient que que $|q - q'| < 1$, q et q' étant entiers, on en déduit que $q = q'$. Par conséquent $r = a - bq = a - bq' = r'$. D'où l'unicité.

Exemple 3 : Prenons un dernier exemple avec $a = -33 < 0$. Cet entier n'est pas multiple de 9 et l'on peut voir en cherchant le plus petit entier naturel r de la forme $r = -33 - 9 \cdot q$ qu'il s'agit de

$$3 = -33 - 9 \cdot (-4).$$

On en déduit donc que le quotient de la division euclidienne de -33 par 9 vaut $q = -4$ et son reste vaut $r = 4$.

9 L'algorithme d'Euclide pour calculer le pgcd

Nous avons vu dans ce qui précède que les nombres premiers constituent les éléments de base de l'arithmétique car tout entier plus grand que 2 est le produit de nombres premiers. Toutefois, nous verrons qu'il est difficile de décider si un nombre est premier ou composé et qu'il est encore plus difficile de trouver les diviseurs premiers d'un entier $n \geq 2$. Au lieu donc de s'intéresser aux diviseurs positifs d'un entier, il est plus fructueux de s'intéresser aux diviseurs en commun à deux entiers a et b. Dans *Le livre 7* des *Éléments*, Euclide a décrit une manière très efficace permettant de calculer le **pgcd** de deux entiers a et b. Je vous rappelle que le mot pgcd(a, b) signifie *le plus grand commun diviseur entre a et b*. Avant

11. Si $0 \leq r < b$ et $0 \leq r' < b$ alors l'écart entre r et r', à savoir $|r' - r|$ est strictement plus petit que b (faites un dessin pour vous en convaincre).

de vous décrire l'algorithme ingénieux d'Euclide, prenons un exemple rapide permettant de comprendre le pgcd.

Exemple : Le pgcd de 70 et 42 vaut 14. En effet, les décompositions en facteurs premiers de 70 et de 42 sont

$$70 = 2 \cdot 5 \cdot 7 \quad \text{et} \quad 42 = 2 \cdot 3 \cdot 7.$$

On voit ainsi que les diviseurs premiers en commun entre 70 et 42 sont 2 et 7. Par conséquent

$$\text{pgcd}(70, 42) = 2 \cdot 7 = 14.$$

Cette méthode fonctionne bien quand il s'agit de calculer le pgcd de nombres petits en taille. Toutefois, trouver la factorisation d'un nombre très grand est un problème réputé difficile et très coûteux en temps. L'algorithme d'Euclide contourne cette difficulté et permet de calculer le pgcd de façon très efficace [12].

9.1 Le pgcd avec soustraction

Nous décrivons dans ce paragraphe l'algorithme d'Euclide avec soustraction. On généralisera par la suite cette idée avec la division euclidienne qui permettra d'avoir un procédé bien plus rapide. Pour calculer le pgcd de deux entiers a et b non tous les deux nuls tels que $a \geq b$, il suffit de remarquer que

$$\text{pgcd}(a, b) = \text{pgcd}(b, a - b).$$

Cette égalité découle du fait que les diviseurs en commun de a et b et ceux de b et $a - b$ sont les mêmes. Pour s'en convaincre, soit d un diviseur en commun entre a et b. Dans ce cas, on écrit $a = a'd$ et $b = b'd$ et par conséquent

$$a - b = a'd - b'd = d(a' - b').$$

Ainsi d divise $a - b$. Réciproquement si d divise b et $a - b$ alors d doit diviser leur somme $b + a - b = a$ (appliquer le même raisonnement si vous n'êtes pas convaincus). Maintenant pour calculer le pgcd, il suffit de réitérer la soustraction afin de tomber sur ce qu'il faut. Un exemple vaut toujours mieux qu'un long discours.

Exemple 1 : Pour les raisons évidentes, on notera (a, b) pour désigner le pgcd de a et b. On souhaite ici calculer $(70, 42)$, mais cette fois-ci avec la remarque euclidienne. Nous avons en effet

$$\begin{aligned}
(70, 42) &= (42, 70 - 42) \\
&= (42, 28) \\
&= (28, 42 - 28) \\
&= (28, 14) \\
&= (14, 28 - 14) \\
&= (14, 14) \\
&= (14, 14 - 14) \\
&= (14, 0) = 14.
\end{aligned}$$

12. On comprendra cette histoire d'efficacité quand on parlera de complexité algorithmique.

Bingo ! On réitérant le procédé de la soustraction on tombe sur le pgcd de 14 et 0. Or de façon générale si $a > 0$ alors

$$(a, 0) = a.$$

Voyez-vous pourquoi ? Cela permet en tout cas d'affirmer que $(14, 0) = 14$.

Exemple 2 : Prenons un deuxième exemple pour se fixer les idées. On souhaite calculer ici le pgcd de 42 et 30. En réitérant les soustractions euclidiennes on obtient

$$\begin{aligned}(42, 30) &= (30, 42-30)\\ &= (30, 12)\\ &= (12, 30-12)\\ &= (12, 18)\\ &= (18, 18-12)\\ &= (18, 6)\\ &= (6, 12)\\ &= (6, 6)\\ &= (6, 0) = 6\end{aligned}$$

Ainsi le pgcd de 42 et 30 vaut 6. On voit alors que ce procédé donne toujours à la fin $(a, 0)$. Cela résulte du fait que l'algorithme d'Euclide produit une suite de nombres entiers naturels décroissante, d'après le principe de la descente infinie de Fermat, cette suite doit bien s'arrêter à un moment donné (à méditer).

9.2 Le pgcd avec division

On peut améliorer l'algorithme d'Euclide avec soustraction en utilisant la division euclidienne. La propriété fondamentale qui permet de faire cela est : si r est le reste de la division euclidienne de a par b alors

$$\text{pgcd}(a, b) = \text{pgcd}(b, r).$$

La preuve de cette égalité est une adaptation de celle avec soustraction (à faire seul du coup). Reprenons ensemble l'exemple 2 mais cette fois avec la division euclidienne. En effet,

$$\begin{aligned}42 = 30 \cdot 1 + 12 &\implies (42, 30) = (30, 12)\\ 30 = 12 \cdot 2 + 6 &\implies (30, 12) = (12, 6)\\ 12 = 6 \cdot 2 + 0 &\implies (12, 6) = (6, 0) = 6.\end{aligned}$$

Pas besoin donc de vous convaincre de la rapidité du procédé avec la division euclidienne. Prenons un deuxième exemple (toujours pour se fixer les idées, je vous invite toutefois à en prendre davantage pour bien comprendre l'algorithme).

Exemple : On souhaite calculer le pgcd de 858 et 770. On commence donc par effectuer la division euclidienne de 858 et 770 et on réitère ensuite la même opération. On obtient ainsi

$$\begin{aligned}858 = 770 \cdot 1 + 88 &\implies (858, 770) = (770, 88)\\ 770 = 88 \cdot 8 + 66 &\implies (770, 88) = (88, 66)\\ 88 = 66 \cdot 1 + 22 &\implies (88, 66) = (66, 22)\\ 66 = 22 \cdot 3 + 0 &\implies (66, 22) = (22, 0).\end{aligned}$$

On voit ainsi que $(858, 770) = 22$ et que le procédé se termine en seulement 4 étapes. Bon courage pour le faire avec la soustraction. Je suis souvent assez curieux, je vous ai donc écrit les deux algorithmes avec Python afin de pouvoir faire la comparaison [13].

```
def pgcd_div(a,b):
    i = 0
    while b != 0:
        a, b = b, a%b
        i += 1
    return a, i

def pgcd_sous(a,b):
    i = 0
    while b != 0:
        if a > b :
            a, b = b, (a - b)
            i += 1
        else:
            a, b = b, a
            a, b = b, (a - b)
            i += 1
    return a, i
```

Le compteur i dans chacun des algorithmes permettra de compter le nombre d'itérations effectuées par le programme afin de calculer le pgcd. En exécutant les deux programmes avec $a = 858$ et $b = 770$ on obtient le résultat suivant.

```
>>> pgcd_div(858, 770)
(22, 4)
>>> pgcd_sous(858, 770)
(22, 13)
```

Ainsi on obtient bien ce qu'on a obtenu à la main, à savoir que le pgcd de 858 et 770 vaut 22, l'algorithme de la division euclidienne s'en sort en 4 étapes tandis que celui avec la soustraction en effectue 13, beaucoup trop ! Je vous invite à aller sur Python afin de faire la comparaison par vous même.

10 L'identité de Bézout et quelques conséquences

Nous passons maintenant à une conséquence importante de l'algorithme d'Euclide. On peut en effet exprimer le pgcd de a et b comme combinaison linéaire de ces deux entiers. En d'autres mots, l'algorithme d'Euclide nous permettra de trouver deux entiers u et v tels que

$$(a, b) = a \cdot u + b \cdot v.$$

Cette identité importante s'appelle l'identité de Bézout, due comme son nom l'indique au mathématicien français Étienne Bézout (ne pas confondre avec Bisous hein !). Un exemple parle toujours bien mieux qu'un long discours.

Exemple 1 : Afin de calculer le pgcd de 42 et 30 nous avons effectué les divisions euclidiennes successives suivantes

$$\begin{aligned} 42 &= 30 \cdot 1 + 12 \\ 30 &= 12 \cdot 2 + 6 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

13. Eh oui les copains, il est grand temps d'apprendre à programmer.

Ainsi le pgcd de 42 et 30 est le dernier reste non nul de cette suite d'opérations. On peut alors remonter ce procédé afin d'exprimer 6 en fonction de 42 et 30. En effet,

$$\begin{aligned} 6 &= 30 - 12 \cdot 2 \\ &= 30 - (42 - 30 \cdot 1) \cdot 2 \quad \text{car } 12 = 42 - 30 \cdot 1 \\ &= 30 - 42 \cdot 2 + 30 \cdot 2 \\ &= 30 \cdot 3 - 42 \cdot 2 \\ &= 30 \cdot 3 + 42 \cdot (-2). \end{aligned}$$

On a donc réussi à exprimer 6 sous la forme $6 = 42 \cdot u + 30 \cdot v$, où ici $u = -2$ et $v = 3$.

Étienne Bézout

Exemple 2 : Reprenons l'exemple avec $a = 858$ et $b = 770$. La suite des divisions euclidiennes est

$$\begin{aligned} 858 &= 770 \cdot 1 + 88 \\ 770 &= 88 \cdot 8 + 66 \\ 88 &= 66 \cdot 1 + 22 \\ 66 &= 22 \cdot 3 + 0. \end{aligned}$$

Là encore le pgcd de 858 et 770 est le dernier reste non nul de cette suite d'opérations. De même, pour trouver u et v tels que $22 = 858u + 770v$, il suffit de remonter ce procédé. En effet,

$$\begin{aligned} 22 &= 88 - 66 \cdot 1 \\ &= 88 - (770 - 88 \cdot 8) \cdot 1 \\ &= 88 \cdot 9 - 770 \cdot 1 \\ &= (858 - 770 \cdot 1) \cdot 9 - 770 \cdot 1 \\ &= 858 \cdot 9 - 770 \cdot 10 \end{aligned}$$

Ainsi $u = 9$ et $v = -10$. Je sens que vous n'êtes pas convaincus. Rien ne vous empêche de vérifier ce calcul pour voir que

$$858 \cdot 9 - 770 \cdot 10 = 7722 - 7700 = 22.$$

Bingo ! Remonter les opérations de l'algorithme d'Euclide s'appelle l'algorithme d'Euclide *étendu*. Notre objectif maintenant est de pouvoir programmer cet algorithme avec Python

et pour se faire, on doit écrire les choses de façon plus formelle.

On aimerait en effet décrire la suite des restes (r_n) obtenus en exécutant l'algorithme d'Euclide. Pour des raisons pratiques, nous prenons $r_0 = a$ et $r_1 = b$. L'algorithme d'Euclide consiste alors à effectuer d'abord la division euclidienne de r_0 par r_1 pour obtenir la relation

$$r_0 = r_1 \cdot q_1 + r_2.$$

La deuxième étape consiste à diviser r_1 par r_2 pour obtenir le reste r_3 vérifiant la relation

$$r_1 = r_2 \cdot q_2 + r_3.$$

La troisième étape de notre fameux algorithme consiste à faire la même chose avec r_2 et r_3, ce qui permettra d'obtenir un nouveau reste r_4 vérifiant la relation

$$r_2 = r_3 \cdot q_3 + r_4.$$

On répète alors ce même procédé jusqu'à ce qu'on obtienne les relations

$$\begin{aligned} r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n \\ r_{n-1} &= r_n \cdot q_n + 0, \end{aligned}$$

où $r_n \neq 0$ désigne le dernier reste non nul. Cela signifie en particulier que r_n est le pgcd tant recherché. Je vous rappelle donc qu'on aimerait écrire r_n en fonction de r_0 et r_1, sous la forme $r_n = r_0 \cdot u + r_1 \cdot v$. Tout d'abord la relation $r_0 = r_1 q_1 + r_2$ implique que $r_2 = r_0 - r_1 q_1$(*). On voit ainsi que r_2 s'écrit comme combinaison de r_0 et r_1. Maintenant la relation $r_1 = r_2 q_2 + r_3$ combinée avec la relation (*) donne

$$\begin{aligned} r_3 &= r_1 - r_2 q_2 \\ &= r_1 - (r_0 - r_1 q_1) q_2 \\ &= r_1(1 + q_1 q_2) - r_0 q_2. \end{aligned}$$

Là encore on voit qu'on peut exprimer r_3 comme combinaison de r_0 et r_1. On effectue la même opération avec r_4 pour obtenir deux entiers u_4 et v_4 tels que $r_4 = r_0 u_4 + r_1 v_4$. On voit alors que plus généralement, le reste r_k s'écrit sous la forme

$$r_k = r_0 u_k + r_1 v_k.$$

Comment cela va-t-il nous aider à programmer notre algorithme ? Pas très évident pour l'instant mais remarquez que l'opération permettant de passer de r_2 à r_3 et ensuite de r_3 à r_4 est essentiellement la même. Cela suggère qu'il existe une relation de récurrence entre u_k et u_{k+1} et entre v_k et v_{k+1}. Regardons ensemble ce que cela donne : on aura besoin des relations suivantes

$$\begin{aligned} r_{k-1} &= r_0 u_{k-1} + r_1 v_{k-1} \\ r_k &= r_0 u_k + r_1 v_k. \end{aligned}$$

On aimerait donc à partir de ces deux relations déduire $r_{k+1} = r_0 u_{k+1} + r_1 v_{k+1}$. En effet, on sait que r_{k-1}, r_k et r_{k+1} sont liés par la relation $r_{k-1} = r_k q_k + r_{k+1}$, ce qui donne que

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_k \\ &= r_0 u_{k-1} + r_1 v_{k-1} - (r_0 u_k + r_1 v_k) q_k \\ &= r_0(u_{k-1} - u_k q_k) + r_1(v_{k-1} - v_k q_k). \end{aligned}$$

On obtient ainsi deux suites (u_k) et (v_k) définies par les relations

$$u_{k+1} = u_{k-1} - u_k q_k \quad \text{et} \quad v_{k+1} = v_{k-1} - v_k q_k.$$

On voit alors qu'elles sont définies par la même relation de récurrence. Toutefois, elles ne donneront pas les mêmes nombres pour une raison d'initialisation. En effet, on sait que $r_0 = r_0 u_0 + r_1 v_0$ ce qui suggère de prendre $u_0 = 1$ et $v_0 = 0$. Par ailleurs $r_1 = r_0 u_1 + r_1 v_1$ ce qui donne donc $u_1 = 0$ et $v_1 = 1$. Prenons un exemple pour comprendre ce qui se passe.

Exemple 3 : On souhaite exprimer ici $6 = (42, 30)$ en fonction de 42 et 30. La suite (u_k) est définie par $u_0 = 1$, $u_1 = 0$ et $u_{k+1} = u_{k-1} - u_k q_k$. De même, la suite (v_k) est définie par $v_0 = 0$, $v_1 = 1$ et $v_{k+1} = v_{k-1} - v_k q_k$. En appliquant d'abord l'algorithme d'Euclide on obtient les divisions successives suivantes

$$\begin{aligned} 42 &= 30 \cdot 1 + 12 \\ 30 &= 12 \cdot 2 + 6 \\ 12 &= 6 \cdot 2 + 0. \end{aligned}$$

On en déduit que $q_1 = 1$ et $q_2 = 2$. Ainsi en utilisant les formules générant (u_k) et (v_k) on obtient

k	q_k	u_k	v_k
0	-	1	0
1	1	0	1
2	2	1	-1
3	-	-2	3

Dans notre cas le dernier reste non nul est r_3 et d'après notre tableau on a $u_3 = -2$ et $v_3 = 3$. Cela implique en particulier que

$$6 = r_3 = r_0 u_3 + r_1 v_3 = 42 \cdot (-2) + 30 \cdot 3.$$

Incroyable, c'est bien la relation obtenue à la main. Je vous invite à appliquer cette méthode avec davantage d'exemples afin de comprendre son fonctionnement. Nous sommes enfin prêts à programmer cette méthode avec Python. Il suffit de savoir programmer une suite récurrente d'ordre 2 (avec deux valeurs initiales). On obtient donc

```
def bezout(a,b):
    u = 1 ; uu = 0
    v = 0 ; vv = 1
    while b != 0:
        q = a // b
        a, b = b, (a % b)
        uu, u = u - q*uu , uu
        vv, v = v - q*vv , vv
    return (a, u, v)
```

En exécutant cet algorithme avec $a = 42$ et $b = 30$ on obtient bien

```
>>> bezout(42, 30)
(6, -2, 3)
>>>
```

Pour récapituler donc, le théorème de Bézout affirme que le pgcd de deux nombres entiers a et b non tous les deux nuls, peut s'écrire comme combinaison de a et de b. En d'autres termes, il existe deux entiers u et v tels que

$$(a,b) = a \cdot u + b \cdot v.$$

Ce théorème sera d'une grande importance pour la suite de notre aventure.

Deux conséquences de l'identité de Bézout :

On décrit dans ce paragraphe quelques conséquences importantes de notre si chère identité de Bézout.

Conséquence 1 : Par définition du pgcd, il s'agit du plus grand diviseur en commun entre deux entiers a et b. En d'autres mots, si r est un diviseur de a et de b alors $r \leq (a,b)$. En réalité, il existe une relation plus forte entre un tel r et le pgcd et l'on peut affirmer que non seulement r est plus petit que le pgcd mais aussi qu'il le divise. Notez alors que le pgcd est plus grand diviseur au sens de la divisibilité, c'est à dire si r divise a et b alors r divise le pgcd. Nous allons utiliser l'identité de Bézout afin de démontrer proprement et convenablement ce résultat, relativement évident intuitivement. Le pgcd de a et b s'écrit sous la forme $(a,b) = a \cdot u + b \cdot v$. Si r est un diviseur en commun à a et b alors on peut écrire $a = r \cdot a'$ et $b = r \cdot b'$. Cela implique donc que

$$\begin{aligned}(a,b) &= a \cdot u + b \cdot v \\ &= r \cdot a' \cdot u + r \cdot b' \cdot v \\ &= r(a'u + b'v).\end{aligned}$$

Le résultat en découle. Remarquez alors qu'on a utilisé à plusieurs reprises dans notre exposé que si a divise b et c alors a divise toute combinaison de b et c de la forme $\alpha b + \beta c$. Modulo ce petit résultat, on aurait pu tout simplement dire que puisque (a,b) est combinaison de a et b alors tout diviseur de a et de b doit diviser son pgcd. Dorénavant, nous utiliserons cette histoire de combinaison sans passer par sa démonstration.

Conséquence 2 : Venons-en maintenant au fameux **Lemme de Gauss**, dû au grand génie [14] *Carl Friedrich Gauss*.

Carl Friedrich Gauss

14. Ce résultat n'est qu'une trivialité comparé aux grands travaux réalisés par son excellence Gauss.

Tout d'abord, je vous rappelle qu'on dit que a et b sont **premiers entre eux** s'ils n'ont aucun diviseur positif en commun sauf 1. Cela revient à dire que le pgcd de a et b vaut $(a,b)=1$ (pourquoi ?). Le lemme de Gauss affirme alors que si a divise $b\cdot c$ et si de plus $(a,b)=1$ alors a doit diviser c. Cela semble aussi intuitivement évident puisque si a et b ne partage aucun diviseur en commun sauf 1 et que a divise le produit bc alors a n'a pas le choix que de diviser c. Toutefois, afin d'éviter les dérapages [15], tout nécessite une démonstration correcte en mathématiques. En effet, $(a,b)=1$ implique d'après l'identité de Bézout l'existence de deux entiers u et v tels que

$$1=a\cdot u+b\cdot v.$$

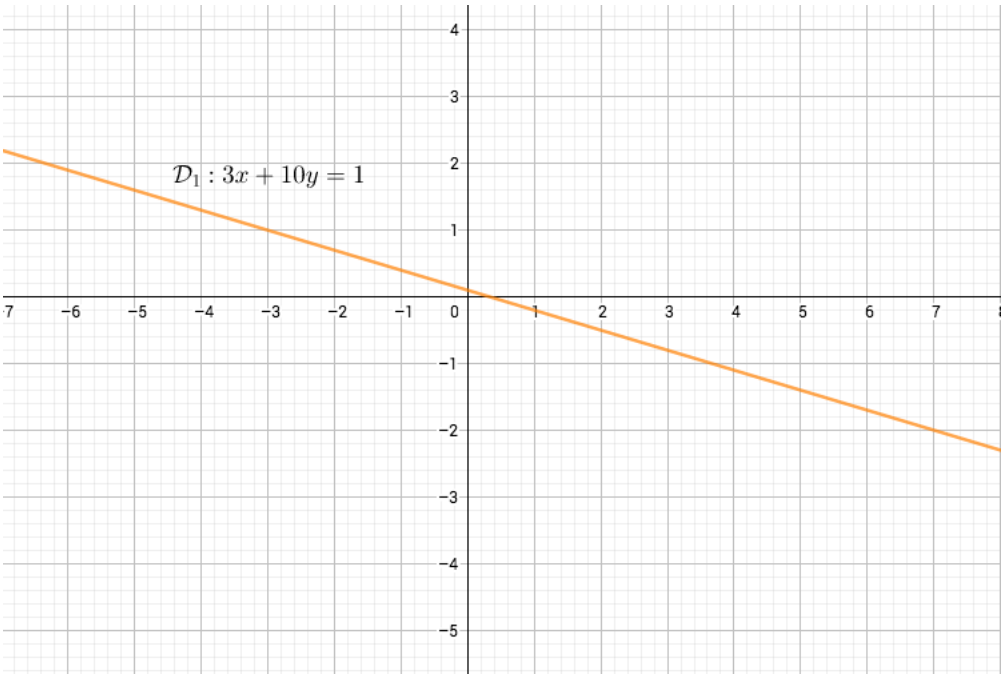
En multipliant cette égalité par c, on obtient $c=c\cdot a\cdot u+(c\cdot b)\cdot v$. Or a divise bc donc a divise c car il divise aussi $c\cdot a\cdot u$.

11 Applications

Nous donnons dans cette section deux applications fondamentales de nos résultats précédents.

11.1 Retour sur les points à coordonnées entières sur une droite

Nous avons vu au début de notre cours que la droite d'équation $3x+10y=1$ contient des points à coordonnées entières comme par exemple le point de coordonnées $(-3,1)$, ou encore le point $(7,-2)$.



En réalité, il existe une infinité de points à coordonnées entières habitant sur cette droite et ils sont de la forme

$$(10k-3,-3k+1).$$

15. Personne n'est à l'abri de déraper mathématiquement, même de très grands mathématiciens.

Nous nous sommes alors demandés si tous les points entiers étaient de cette forme et nous pouvons maintenant répondre à cette question. En effet, $(-3,1)$ est un point sur notre droite et si (x,y) est un point à coordonnées entières situé sur cette même droite alors

$$\begin{cases} 3x+10y & =1 \\ 3\cdot(-3)+10\cdot 1 & =1 \end{cases}$$

On soustrait alors la deuxième équation à la première pour obtenir $3(x+3)+10(y-1)=0$ ou encore

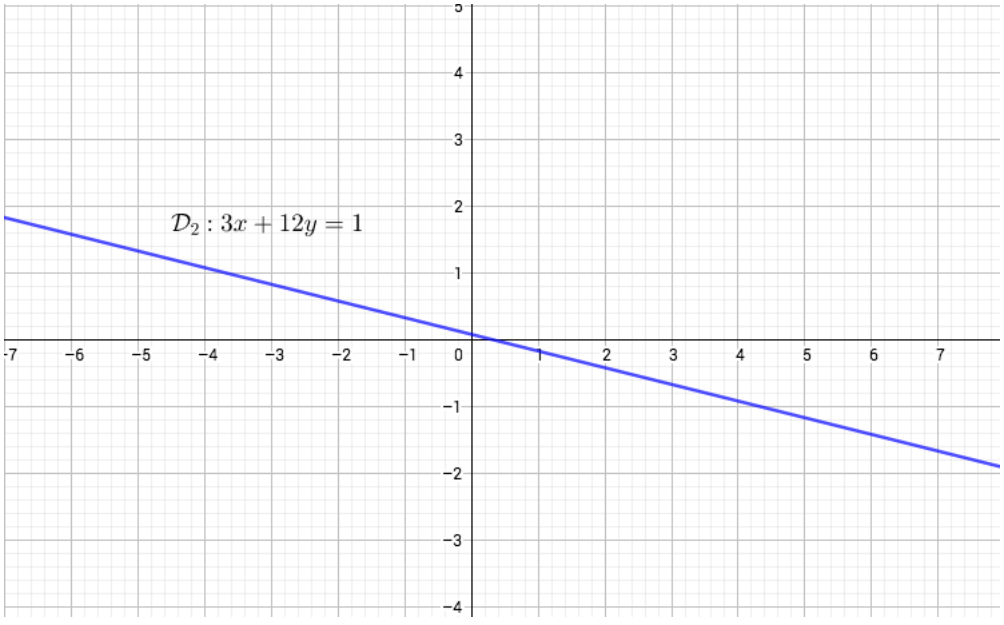
$$3(x+3)=10(1-y).$$

Puisque tout se passe dans $\mathbb{Z}$, cette égalité implique que 3 divise $10(1-y)$. Or 3 et 10 sont premiers entre eux, donc d'après le lemme de notre bon vieux Gauss 3 doit diviser $1-y$. Autrement dit, il existe un entier k tel que $1-y=3k$, ce qui signifie que $y=-3k+1$! Oh, incroyable ! Maintenant l'égalité $3(x+3)=10(1-y)$ devient

$$3(x+3)=10\cdot 3k,$$

en simplifiant par 3 de part et d'autre on obtient $x=10k-3$, qui est la forme voulue pour x. Pour conclure, nous sommes partis d'un couple $(x,y)\in\mathbb{Z}^2$ solution de $3x+10y=1$ et nous avons montré qu'il est forcément de la forme $(10k-3,-3k+1)$. D'où la réponse à notre question, toutefois une deuxième question me saute aux yeux personnellement (j'espère que c'est le cas pour vous aussi). Nous avons en effet utiliser la solution particulière $(-3,1)$ pour résoudre totalement notre équation mais comment trouver une solution particulière à n'importe quelle équation du type $ax+by=c$ et est-ce toujours possible ?

Nous avons vu ensemble que la droite d'équation $3x+12y=1$ n'abrite aucun point à coordonnées entières car dans ce cas on obtient l'égalité $3(x+4y)=1$ ce qui signifie que 3 divise 1, contradiction.



Plus généralement, une équation de la forme $ax+by=c$ admet une solution entière si et seulement si le pgcd de a et b divise c. En effet, le sens direct est relativement évident car si (x_0,y_0) est une solution entière de notre équation alors $ax_0+by_0=c$. Puisque le

pgcd de a et b divise a et b, il divise toute combinaison linéaire de ces deux entiers, en particulier l'entier c. Réciproquement, si (a,b) divise c alors l'équation $ax+by=c$ admet une solution entière. En effet, d'après Bézout on peut toujours trouver deux entiers u et v tels que $(a,b)=a\cdot u+b\cdot v$. Ainsi puisque (a,b) divise c, on peut écrire $c=c'\cdot(a,b)$, donc en multipliant par c' on obtient

$$\begin{aligned} c=c'(a,b) &= c'au+c'bv \\ &= a(c'u)+b(c'v). \end{aligned}$$

On en déduit donc que le couple $(c'u,c'v)$ est solution entière de l'équation $ax+by=c$. Le tout repose donc sur l'algorithme d'Euclide étendu qui permet de trouver les nombres u et v. Sans perte de généralité, nous pouvons supposer $(a,b)=1$ [16]. Dans ce cas, quand on obtient un point particulier (x_0,y_0) sur la droite d'équation $ax+by=c$, on obtient les autres points de la façon suivante. Si (x,y) est un point à coordonnées entières habitant la droite, alors

$$\begin{cases} ax+by &= c \\ ax_0+by_0 &= c \end{cases}$$

On soustrait la deuxième équation de la première pour obtenir $a(x-x_0)+b(y-y_0)=0$, autrement

$$a(x-x_0)=b(y_0-y).$$

Là encore puisque cette égalité se passe dans $\mathbb{Z}$, a divise $b(y_0-y)$. Or a et b sont premiers entre eux car $(a,b)=1$, le lemme de Gauss implique du coup que a divise y_0-y, d'où l'existence d'un entier k tel que $y_0-y=a\cdot k$ ou encore que $y=-a\cdot k+y_0$. L'égalité $a(x-x_0)=b(y_0-y)$ implique alors que

$$a(x-x_0)=b\cdot ak,$$

donc en simplifiant par a, $x=bk+x_0$. Ainsi les solutions de l'équation $ax+by=c$ doivent être de la forme

$$(x_0+bk,y_0-ak), \quad \text{où } k\in\mathbb{Z}.$$

Réciproquement, on voit bien que

$$\begin{aligned} a(x_0+bk)+b(y_0-ak) &= ax_0+by_0+abk-abk \\ &= c. \end{aligned}$$

Voilà donc pour la théorie, prenons maintenant un exemple concret.

Exemple : On souhaite résoudre dans $\mathbb{Z}^2$ l'équation $25x+13y=3$. Les entiers 25 et 13 n'ont aucun diviseur positif en commun sauf 1 donc $(25,13)=1$, or 1 divise 3 donc d'après ce qui précède notre équation admet une solution particulière et par conséquent une infinité de solution. Commençons d'abord par exprimer $(25,13)$ en fonction de 25 et 13. La suite des opérations de l'algorithme d'Euclide est

$$\begin{aligned} 25 &= 13\cdot 1+12 \\ 13 &= 12\cdot 1+1 \\ 12 &= 1\cdot 12+0 \end{aligned}$$

16. Dans le cas contraire, on divise l'équation par (a,b).

Ainsi en remontant ces opérations on obtient

$$\begin{aligned} 1 &= 13 - 12 \cdot 1 \\ &= 13 - (25 - 13 \cdot 1) \cdot 1 \\ &= 13 \cdot 2 + 25 \cdot (-1). \end{aligned}$$

En multipliant par 3 on obtient $25 \cdot (-3) + 13 \cdot 6 = 3$, ce qui nous donne $(-3, 6)$ comme solution particulière de notre équation $25x + 13y = 3$. D'après notre petite théorie, les autres solutions sont de la forme

$$(-3 + 13k, 6 - 25k), \quad \text{où } k \in \mathbb{Z}.$$

11.2 Racines rationnelles d'un polynôme

11.2.1 Ensembles de nombres et racines de polynômes

Le premier ensemble de nombres que l'on rencontre dans la nature et en arithmétique est l'ensemble des entiers naturels

$$\mathbb{N} = \{0, 1, 2, 3, \cdots\}.$$

Les entiers naturels servent essentiellement à compter les objets. Toutefois, pour nos utilisations mathématiques, on se heurte très rapidement à des difficultés conceptuelles en travaillant uniquement dans $\mathbb{N}$. Par exemple l'équation

$$2 + x = 5$$

admet une solution dans $\mathbb{N}$, à savoir $x = 3$. Néanmoins, l'équation $5 + x = 2$, semblable à la première n'admet pas de solution dans $\mathbb{N}$, pour la simple raison, qu'en travaillant chez les entiers naturels $5 + x \geq 5$ et donc ne pourra jamais atteindre 2. Nous avons donc besoin d'un ensemble plus grand que $\mathbb{N}$, celui des entiers relatifs qu'on dénote

$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\},$$

où la lettre $\mathbb{Z}$ fait référence ici au mot *Zahlen*, signifiant nombres en allemand. L'équation $5 + x = 2$ devient alors résoluble dans $\mathbb{Z}$ et sa solution vaut $x = -3$. Toutefois, l'équation $2x = 4$ admet une solution dans $\mathbb{Z}$ mais l'équation similaire $4x = 2$ n'en admet pas. Nous avons donc besoin de construire un ensemble de nombres plus grand que $\mathbb{Z}$, à savoir cette fois-ci l'ensemble des nombres rationnels (les fractions)

$$\mathbb{Q} = \left\{ \frac{p}{q}, (p, q) \in \mathbb{Z} \times \mathbb{N}^* \right\}.$$

L'ensemble $\mathbb{Q}$ suffit-il alors pour résoudre toute équation à coefficients entiers ? L'équation $x^2 = 2$ est à coefficients entiers et pourtant elle n'admet pas de solutions dans $\mathbb{Q}$, puisqu'on a vu ensemble que $\sqrt{2}$ n'est pas un nombre rationnel. On aimerait alors étendre $\mathbb{Q}$ à un ensemble plus grand permettant de résoudre par exemple les équations du type $x^2 = a$.

Pour ce faire, nous allons utiliser le développement décimal d'un nombre. Le développement décimale d'une fraction est toujours périodique, mais mieux encore tout nombre avec un développement décimal périodique est forcément une fraction. Par exemple,

$$\frac{3}{7} = 0.428571\ 428571\ 428571 \cdots$$

on voit aisément que $3/7$ admet un développement décimal périodique et que plus généralement le développement décimale de n'importe quelle fraction est périodique à partir d'un certain rang (pourquoi ?). Réciproquement, tout nombre dont le développement décimal est périodique à partir d'un certain rang est une fraction. Regardons ensemble ce qui se passe sur un exemple. Soit x le nombre

$$x = 0.12345\ 345\ 345\ldots.$$

En multipliant x par 10^2 on obtient

$$10^2 x = 12.345\ 345\ 345\ldots.$$

De même, en le multipliant par 10^5 on obtient $10^5 x = 12345.345\ 345\ldots$. L'égalité

$$(10^5 - 10^2)x = 12345 - 12$$

en découle et il s'en suit donc que x est une fraction égale à $12333/99900$. Ce procédé se généralise bien facilement et notre réciproque tombe ainsi comme une pomme mûre. Notez alors que les premières décimales de $\sqrt{2}$ sont

$$\sqrt{2} = 1.41421356237309504880168872420969807856967187537694807317667 9\cdots$$

et que a priori ce développement n'est pas périodique. En réalité il ne peut pas l'être car on a montré que $\sqrt{2}$ ne s'écrit pas sous la forme d'une fraction et que seules les fractions admettent cette propriété.

Cette remarque suggère une idée d'une possible extension de $\mathbb{Q}$. Puisque ce dernier est l'ensemble des nombres dont le développement décimal est périodique à partir d'un certain rang, il suffit de prendre de façon informelle l'ensemble de tous les développements décimaux possibles. On obtient ainsi

$$\mathbb{R} = \text{ensemble de tous les développements décimaux.}$$

L'ensemble des nombres réels permet donc de résoudre davantage d'équations, même à coefficients réels. On sait par exemple que si $\Delta = b^2 - 4ac \geq 0$, l'équation générale

$$ax^2 + bx + c = 0, \quad \text{où } a \neq 0,$$

admet deux solutions (comptées avec multiplicité), à savoir $x_{1,2} = \pm(-b \pm \sqrt{\Delta})/2a$. On se demande alors très naturellement si maintenant toutes les équations à coefficients réels admettent des solutions dans $\mathbb{R}$. Vous n'êtes pas sans savoir que l'équation $x^2+1 = 0$ n'admet pas de solution réelle, car dans $\mathbb{R}$, $x^2 + 1 \geq 1$ et donc n'atteint jamais 0. Nous avons là encore besoin de créer de façon un peu artificielle un ensemble de nombres contenant $\mathbb{R}$ et un nombre imaginaire i vérifiant

$$i^2 = -1.$$

Autrement dit, on considère un nombre i solution de l'équation $x^2 + 1 = 0$. On obtient à partir de là l'ensemble des nombres complexes $\mathbb{C}$. Nous avons ainsi introduit plusieurs ensembles de nombres tels que

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

afin de pouvoir résoudre davantage d'équations. Mais ce procédé s'arrêtera-t-il un jour ? Ou doit-on encore construire un ensemble plus grand que $\mathbb{C}$ contenant des racines d'équations à coefficients dans $\mathbb{C}$. Aussi surprenant que cela puisse paraître, $\mathbb{C}$ contient les racines de n'importe quelle équation à coefficients dans cet ensemble ! Et donc on n'a plus besoin d'élargir nos ensembles afin de résoudre nos équations. Ce fameux théorème s'appelle le **théorème fondamental de l'algèbre** et il dit que tout polynôme non constant à coefficients dans $\mathbb{C}$ admet une racine dans $\mathbb{C}$. On dit alors que $\mathbb{C}$ est algébriquement clos. La preuve de ce théorème dépasse un peu le cadre de notre cours.

11.2.2 Racines entières et rationnelles d'un polynôme

Dans la suite nous nous intéressons aux ensembles $\mathbb{Z}$ et $\mathbb{Q}$. Nous souhaitons trouver les solutions entières du polynôme

$$P(x) = 3x^3 - 11x^2 - 24x + 20.$$

Si $n \in \mathbb{Z}$ tel que $P(n) = 0$ alors on peut affirmer que

$$n(3n^2 - 11n - 24) = -20.$$

Puisque tout se passe dans $\mathbb{Z}$, cela signifie que si n est racine de P alors n doit diviser (-20) ou encore que

$$n \in \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\}$$

Il s'agit donc d'essayer un nombre fini de valeurs pour voir si l'une d'entre elles est solution de notre équation. Après plusieurs essais, on voit que les solutions de P habitant dans $\mathbb{Z}$ sont (-2) et 5. Or P est de degré 3, donc il doit admettre une troisième solution, possiblement vivant dans $\mathbb{Q}$. Soit donc $r = p/q \in \mathbb{Q}$ tel que $P(r) = 0$ et $(p, q) = 1$. Cette dernière égalité s'écrit

$$3\left(\frac{p}{q}\right)^3 - 11\left(\frac{p}{q}\right)^2 - 24\left(\frac{p}{q}\right) + 20 = 0.$$

On obtient donc en multipliant par q^3 l'égalité dans $\mathbb{Z}$, $3p^3 - 11p^2q - 24pq^2 + 20q^3 = 0$. Par conséquent

$$p(3p^2 - 11pq - 24q^2) = -20q^3 \quad \text{et} \quad q(20q^2 - 24pq - 11p^2) = -3p^3.$$

Ceci signifie que p divise $-20q^3$ et q divise $-3p^3$. Je prétends que c'est quasiment fini puisque d'après le lemme de Gauss p doit diviser -20 et q doit de son côté diviser (-3). On en déduit donc que

$$p \in \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\} \quad \text{et} \quad q \in \{\pm 1, \pm 3\}.$$

Après divers essais, on voit que la dernière solution de P est $r = 2/3$. Notez alors qu'on aurait pu trouver cette dernière solution bien plus facilement en effectuant la division euclidienne du polynôme P par le polynôme $(x + 2)(x - 5)$ et P s'écrit ainsi sous la forme

$$P(x) = 3(x - 2)(x + 5)(x - 2/3).$$

Cet exemple se généralise facilement et je vous invite à démontrer que si P est un polynôme de degré $n \geq 1$ défini par l'expression

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

où $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ et si $r = p/q$ est une fraction irréductible vérifiant $P(r) = 0$ alors le lemme de Gauss nous permet d'affirmer que p divise a_0 et que q divise a_n.

Pour finir cette section, nous donnons une preuve alternative de l'irrationalité de $\sqrt{2}$ en montrant que le polynôme $P(x) = x^2 - 2$ n'admet pas de racines rationnelles. En effet, si $r = p/q$ est irréductible telle que $P(r) = 0$ alors p et q doivent diviser respectivement 2 et 1. Ainsi $r = \pm 2$, mais $2^2 - 2 = (-2)^2 - 2 = 2 \neq 0$. Ainsi P n'admet aucune solution rationnelle. Ceci achève notre super preuve.